PCT/JP03/10016

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

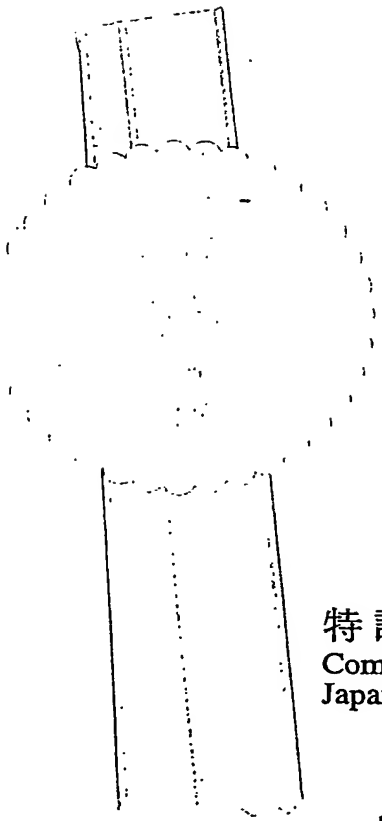
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　７月２５日

出願番号
Application Number: 特願２００３－２８０３７５

[ST. 10/C]: [ＪＰ２００３－２８０３７５]

出願人
Applicant(s): キヤノン株式会社



２００３年１０月２４日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

【書類名】　特許願
【整理番号】　255800
【提出日】　平成15年 7月25日
【あて先】　特許庁長官殿
【国際特許分類】　H04N 5/00
【発明者】
　【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
　【氏名】　皆川　智徳
【特許出願人】
　【識別番号】　000001007
　【氏名又は名称】　キヤノン株式会社
【代理人】
　【識別番号】　100090273
　【弁理士】
　【氏名又は名称】　國分　孝悦
　【電話番号】　03-3590-8901
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-228950
　【出願日】　平成14年 8月 6日
【手数料の表示】
　【予納台帳番号】　035493
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9705348

【書類名】特許請求の範囲
【請求項１】
印刷データを含んだ印刷ジョブを、通信媒体を介して指定の画像形成装置に送信して、前記指定の画像形成装置により前記印刷データを印刷するように制御する印刷制御装置であって、
前記印刷ジョブの印刷が指定された画像形成装置で復号化することが可能な暗号化方法で前記印刷データを暗号化する印刷データ暗号化手段と、
前記画像形成装置に対応する出力先を示す情報を取得する取得手段と、
前記取得手段が取得した出力先を示す情報を復号する復号手段とを備えた、印刷制御装置。
【請求項２】
前記印刷データから特徴量を算出する特徴量算出手段と、
前記特徴量算出手段により算出された特徴量を前記印刷ジョブに含めて前記通信媒体を介して前記指定の画像形成装置に送信する印刷ジョブ送信手段とをさらに有する、請求項１に記載の印刷制御装置。
【請求項３】
前記取得手段が取得した出力先を示す情報は、印刷先のポート、又は、ユニフォーム・リソース・アイデンティファイア（ＵＲＩ）である、請求項１または２に記載の印刷制御装置。
【請求項４】
前記印刷データ暗号化手段は、公開鍵暗号法に基づく暗号化処理を行なう公開鍵暗号化手段として機能し、前記公開鍵暗号法に基づいて、前記印刷データの印刷が指定された画像形成装置の公開鍵を用いて、前記印刷データを暗号化する、請求項１～３の何れか１項に記載の印刷制御装置。
【請求項５】
前記印刷データの印刷が指定された画像形成装置と共通の秘密鍵を作成する秘密鍵作成手段と、
前記秘密鍵作成手段により作成された秘密鍵を暗号化する秘密鍵暗号化手段と、
前記秘密鍵暗号化手段により暗号化された秘密鍵を前記印刷ジョブに含めて、前記通信媒体に送信する印刷ジョブ送信手段とをさらに有し、
前記印刷データ暗号化手段は、共通鍵暗号法に基づく暗号化処理を行なう共通鍵暗号化手段として機能し、前記共通鍵暗号法に基づいて前記秘密鍵作成手段により作成された秘密鍵で前記印刷データを暗号化し、
前記秘密鍵暗号化手段は、公開鍵暗号法に基づく暗号化処理を行なう公開鍵暗号化手段として機能し、前記公開鍵暗号法に基づく暗号化処理を行ない、前記印刷データの印刷が指定された画像形成装置の公開鍵で前記秘密鍵を暗号化する、請求項１に記載の印刷制御装置。
【請求項６】
前記特徴量算出手段により算出された特徴量に対して、公開鍵暗号法に基づく暗号化処理を適用して、自身のプライベートキーで暗号化し、デジタル署名を作成するデジタル署名作成手段をさらに有し、
前記印刷ジョブ送信手段は、前記デジタル署名作成手段により作成されたデジタル署名を、前記特徴量算出手段により算出された特徴量の代わりに前記印刷ジョブに含めて前記通信媒体に送信する、請求項２～４の何れか１項に記載の印刷制御装置。
【請求項７】
前記画像形成装置の情報を管理する画像形成装置管理サーバに問い合わせて、前記印刷データを印刷する画像形成装置を選択する画像形成装置選択手段と、
前記印刷データを印刷するように指定された画像形成装置の情報を前記画像形成装置管理サーバから取得する画像形成装置情報取得手段とをさらに有する、請求項１～６の何れか１項に記載の印刷制御装置。

【請求項８】
前記画像形成装置情報取得手段は、前記印刷データの印刷が指定された画像形成装置の暗号鍵及びアドレスを前記画像形成装置管理サーバから取得し、
前記印刷データ暗号化手段は、前記画像形成装置情報取得手段により取得した画像形成装置の暗号鍵を用いて前記印刷データを暗号化して、前記画像形成装置情報取得手段により取得した画像形成装置のアドレスに直接送信する、請求項７に記載の印刷制御装置。
【請求項９】
前記印刷データ暗号化手段は、前記画像形成装置管理サーバの暗号鍵を取得して前記印刷データを暗号化し、前記暗号化した印刷データを前記画像形成装置管理サーバに送信する、請求項７または８に記載の印刷制御装置。
【請求項１０】
前記画像形成装置選択手段が該当する画像形成装置を選択するために必要な条件を前記画像形成装置情報取得手段が前記画像形成装置管理サーバに送信することで、前記画像形成装置選択手段が該当する画像形成装置を選択する、請求項７～９の何れか１項に記載の印刷制御装置。
【請求項１１】
前記画像形成装置管理サーバが該当する画像形成装置を絞り込むために必要な条件を前記画像形成装置情報取得手段が前記画像形成装置管理サーバに送信することで、前記画像形成装置管理サーバで該当する画像形成装置を絞り込ませるようにし、前記該当する画像形成装置を絞り込んだ画像形成装置管理サーバと前記画像形成装置選択手段とが対話的な通信を行なうことで前記印刷データの印刷を行なう画像形成装置を選択するようにした、請求項７～９の何れか１項に記載の印刷制御装置。
【請求項１２】
通信媒体を介して受信した印刷ジョブに含まれる暗号化された印刷データを印刷する画像形成装置であって、
前記暗号化された印刷データを所定の複号化方法で復号化する印刷データ復号化手段と、
前記受信した印刷ジョブから特徴量を取得する特徴量取得手段と、
前記印刷データ復号化手段により復号化された印刷データから特徴量を算出する特徴量算出手段と、
画像形成装置に対応する出力先を示す情報を暗号化して転送する転送手段と、
前記特徴量算出手段により算出された特徴量と、前記特徴量取得手段によって取得された特徴量とを比較し、両者が一致していることを確かめることで、前記暗号化された印刷データに破損や改ざんが無いことを確認する印刷データ確認手段とを有する、画像形成装置。
【請求項１３】
前記印刷データ復号化手段は、公開暗号法に基づく復号化処理を行なう公開鍵復号化手段として機能し、前記復号化処理を適用して、前記暗号化された印刷データを、自身のプライベートキーを用いて復号化して、前記印刷データを取得する、請求項１２に記載の画像形成装置。
【請求項１４】
前記受信した印刷ジョブから、暗号化された秘密鍵を取り出す秘密鍵取り出し手段と、
前記秘密鍵取り出し手段により取り出された暗号化された秘密鍵に対し、公開鍵復号法に基づく復号化処理を行なって自身のプライベートキーで復号化して秘密鍵を取得する秘密鍵取得手段とを有し、
前記印刷データ復号化手段は、共通鍵暗号法に基づく復号化処理を行なう共通鍵復号化手段として機能し、前記共通鍵暗号法を適用して、前記暗号化された印刷データを前記秘密鍵で復号化して印刷データを取得する、請求項１２または１３に記載の画像形成装置。
【請求項１５】
前記受信した印刷ジョブから、デジタル署名を取り出すデジタル署名取り出し手段を有

し、
前記特徴量取得手段は、前記デジタル署名取り出し手段により取り出したデジタル署名を、前記印刷ジョブの送信元の公開鍵を用いて公開鍵復号法に基づき復号化して特徴量を取得し、
前記印刷データ確認手段は、前記印刷データ復号化手段により復号化した印刷データから算出した特徴量と、前記特徴量取得手段によって取得した特徴量とを比較し、両者が一致していることを確かめることで、送信元が特定の画像形成装置ドライバであり、且つ前記暗号化された印刷データに破損や改ざんが無いことを確認する、請求項１２～１４の何れか１項に記載の画像形成装置。
【請求項１６】
通信媒体を介して接続された画像形成装置の情報を管理する画像形成装置管理サーバであって、
前記通信媒体を介して接続された使用可能な画像形成装置の設置位置や能力、及び各画像形成装置の暗号鍵を含む情報の一覧を所持する情報所持手段と、
前記画像形成装置の印刷制御を行なう印刷制御装置からの問合せに応じて、前記情報所持手段により所持されている情報の一覧を参照して、印刷データの印刷を行なうのに適した画像形成装置を選択する画像形成装置選択手段と、
前記印刷制御装置からの問合せに応じて、前記画像形成装置選択手段により選択された画像形成装置の暗号鍵やアドレス情報を取得する画像形成装置情報取得手段と、
前記印刷制御装置から受信した暗号化された印刷データを、前記情報所持手段により所持されている暗号鍵で復号化し、さらに、前記復号化した印刷データを前記画像形成装置情報取得手段により取得した画像形成装置の暗号鍵で再度暗号化し、前記再度暗号化した印刷データを、前記画像形成装置情報取得手段により取得したアドレスに送信する画像形成装置情報送信手段とを有する、画像形成装置管理サーバ。
【請求項１７】
印刷データを含んだ印刷ジョブを、通信媒体を介して指定の画像形成装置に送信して、前記指定の画像形成装置により前記印刷データを印刷するように制御する印刷制御方法であって、
前記印刷ジョブの印刷が指定された画像形成装置で復号化することが可能な暗号化方法で前記印刷データを暗号化する印刷データ暗号化処理を行ない、前記画像形成装置に対応する出力先を示す情報を取得し、取得した出力先を示す情報を復号する、印刷制御方法。
【請求項１８】
前記印刷データから特徴量を算出する特徴量算出処理と、
前記特徴量算出処理により算出された特徴量を前記印刷ジョブに含めて前記通信媒体を介して前記指定の画像形成装置に送信する印刷ジョブ送信処理とをさらに行なう、請求項１７に記載の印刷制御方法。
【請求項１９】
前記印刷データ暗号化処理は、前記印刷データの印刷が指定された画像形成装置の公開鍵を用いて、公開鍵暗号法に基づく暗号化処理である公開鍵暗号化処理を行なって、前記印刷データを暗号化する、請求項１７または１８に記載の印刷制御方法。
【請求項２０】
前記印刷データの印刷が指定された画像形成装置と共通の秘密鍵を作成する秘密鍵作成処理と、
前記秘密鍵作成処理により作成された秘密鍵を暗号化する秘密鍵暗号化処理と、
前記秘密鍵暗号化処理により暗号化された秘密鍵を前記印刷ジョブに含めて、前記通信媒体に送信する印刷ジョブ送信処理とをさらに行ない、
前記印刷データ暗号化処理は、前記秘密鍵作成処理により作成された秘密鍵を用いて、共通鍵暗号法に基づく暗号化処理である共通鍵暗号化処理を行なって、前記印刷データを暗号化し、
前記秘密鍵暗号化処理は、前記印刷データの印刷が指定された画像形成装置の公開鍵を

用いて、公開鍵暗号法に基づく暗号化処理である公開鍵暗号化処理を行なって、前記秘密鍵を暗号化する、請求項１７に記載の印刷制御方法。

【請求項２１】

前記特徴量算出処理により算出された特徴量に対して、プライベートキーを用いて公開鍵暗号法に基づく暗号化処理を行なって暗号化し、デジタル署名を作成するデジタル署名作成処理をさらに行ない、

前記印刷ジョブ送信処理は、前記デジタル署名作成処理により作成されたデジタル署名を、前記特徴量算出処理により算出された特徴量の代わりに前記印刷ジョブに含めて前記通信媒体に送信する、請求項１８または１９に記載の印刷制御方法。

【請求項２２】

前記画像形成装置の情報を管理する画像形成装置管理サーバに問い合わせて、前記印刷データを印刷する画像形成装置を選択する画像形成装置選択処理と、

前記印刷データの印刷が指定された画像形成装置の情報を前記画像形成装置管理サーバから取得する画像形成装置情報取得処理とをさらに行なう、請求項１７～２１の何れか１項に記載の印刷制御方法。

【請求項２３】

前記画像形成装置情報取得処理は、前記印刷データの印刷が指定された画像形成装置の暗号鍵やアドレスを前記画像形成装置管理サーバから取得し、

前記印刷データ暗号化処理は、前記画像形成装置情報取得処理により取得した画像形成装置の暗号鍵を用いて前記印刷データを暗号化して、前記画像形成装置情報取得処理により取得した画像形成装置のアドレスに、前記暗号化した印刷データを直接送信する、請求項２２に記載の印刷制御方法。

【請求項２４】

前記印刷データ暗号化処理は、前記画像形成装置管理サーバの暗号鍵を取得して前記印刷データを暗号化し、前記暗号化した印刷データを前記画像形成装置管理サーバに送信する、請求項２２に記載の印刷制御方法。

【請求項２５】

前記画像形成装置選択処理で該当する画像形成装置を選択するために必要な条件を、前記画像形成装置情報取得処理で前記画像形成装置管理サーバに送信することで、前記画像形成装置選択処理により該当する画像形成装置を選択する、請求項２２～２４の何れか１項に記載の印刷制御方法。

【請求項２６】

前記画像形成装置管理サーバで該当する画像形成装置を絞り込むために必要な条件を、前記画像形成装置情報取得処理で前記画像形成装置管理サーバに送信することで、前記画像形成装置管理サーバで該当する画像形成装置を絞り込ませるようにし、前記画像形成装置選択処理で、前記該当する画像形成装置を絞り込んだ画像形成装置管理サーバと対話的な通信を行なうことで前記印刷データの印刷を行なう画像形成装置を選択するようにした、請求項２２～２４の何れか１項に記載の印刷制御方法。

【請求項２７】

前記受信した印刷ジョブから特徴量を取得する特徴量取得処理と、

前記暗号化された印刷データを復号化し、復号化した印刷データから特徴量を算出する特徴量算出処理と、

前記画像形成装置に対応する出力先を示す情報を暗号化して転送する転送処理と、

前記特徴量算出処理により算出された特徴量と、前記特徴量取得処理によって取得された特徴量とを比較し、両者が一致していることを確かめることで、前記暗号化された印刷データに破損や改ざんが無いことを確認する印刷データ確認処理とをさらに行なう、請求項１７～２６の何れか１項に記載の印刷制御方法。

【請求項２８】

プライベートキーを用いて公開暗号法に基づく復号化処理である公開鍵復号化処理を行なって、前記暗号化された印刷データを復号化し、前記印刷データを取得する、請求項２

７に記載の印刷制御方法。
【請求項２９】
前記受信した印刷ジョブから、暗号化された秘密鍵を取り出す秘密鍵取り出し処理と、
前記秘密鍵取り出し処理により取り出した暗号化された秘密鍵に対し、公開鍵復号法に基づく復号化処理を行なって自身のプライベートキーで復号化し、秘密鍵を取得する秘密鍵取得処理とを行ない、
共通鍵暗号法に基づく復号化処理である共通鍵復号化処理を行なって、前記暗号化された印刷データを前記秘密鍵で復号化し、印刷データを取得する、請求項２７または２８に記載の印刷制御方法。
【請求項３０】
前記受信した印刷ジョブから、デジタル署名を取り出すデジタル署名取り出し処理を行ない、
前記特徴量取得処理は、前記デジタル署名取り出し処理により取り出したデジタル署名を、前記印刷ジョブの送信元の公開鍵を用いて公開鍵復号法に基づき復号化して特徴量を取得し、
前記印刷データ確認処理は、前記復号化した印刷データから算出した特徴量と、前記特徴量取得処理によって取得した特徴量とを比較し、両者一致していることを確かめることで、送信元が特定の画像形成装置ドライバであり、且つ前記暗号化された印刷データに破損や改ざんが無いことを確認する、請求項２７～２９の何れか１項に記載の印刷制御方法。
【請求項３１】
前記通信媒体を介して接続された使用可能な画像形成装置の設置位置や能力、及び各画像形成装置の暗号鍵を含む情報の一覧を所持する情報所持処理と、
前記画像形成装置の印刷制御を行なう印刷制御装置からの問合せに応じて、前記情報所持処理により所持されている情報の一覧を参照して、印刷データの印刷を行なうのに適した画像形成装置を選択する選択処理と、
前記印刷制御装置からの問合せに応じて、前記選択処理により選択された画像形成装置の暗号鍵やアドレス情報を取得する情報取得処理と、
前記印刷制御装置から受信した暗号化された印刷データを、前記情報所持処理により所持されている暗号鍵で復号化し、さらに、前記復号化した印刷データを前記情報取得処理により取得した画像形成装置の暗号鍵で再度暗号化し、前記再度暗号化した印刷データを、前記情報取得処理により取得した画像形成装置のアドレスに送信する画像形成装置情報送信処理とを行なう、請求項１７～３０の何れか１項に記載の印刷制御方法。
【請求項３２】
印刷データを含んだ印刷ジョブを、通信媒体を介して指定の画像形成装置に送信して、前記指定の画像形成装置により前記印刷データを印刷するように制御するに際し、
前記印刷ジョブの印刷が指定された画像形成装置で復号化することが可能な暗号化方法で前記印刷データを暗号化する印刷データ暗号化処理と、
前記画像形成装置に対応する出力先を示す情報を取得する取得処理と、
前記取得処理で取得した出力先を示す情報を復号する復号処理と、
をコンピュータに実行させるコンピュータプログラムを記憶した、コンピュータ読取り可能な記憶媒体。

【書類名】明細書
【発明の名称】印刷制御装置、画像形成装置、画像形成装置管理サーバ、印刷制御方法、及びコンピュータ読み取り可能な記憶媒体
【技術分野】
【０００１】
本発明は、印刷制御装置、画像形成装置、画像形成装置管理サーバ、印刷制御方法、及びコンピュータ読み取り可能な記憶媒体に関し、特に、インターネットやネットワークなどの通信媒体を経由して印刷データの印刷を行なうために用いると好適なものである。
【背景技術】
【０００２】
従来からホストコンピュータから画像形成装置の一例であるプリンタに印刷を行なう際の手法として、ホストコンピュータとプリンタとをケーブルで直接つなぐスタンドアローン接続と、ホストコンピュータとプリンタとを、ネットワークを介してつなぐネットワーク接続を行なって離れた場所にあるプリンタを利用するネットワーク接続とがある。
【０００３】
これらの手法のうち、前記ネットワーク接続を行なってネットワーク経由で印刷するネットワーク印刷では、ネットワーク（インターネット）でつながった先のプリンタにも印刷することができるという利点を有している。そして、前記ネットワーク印刷では、大型の高速プリンタや高価なカラープリンタを複数の端末装置で共有したり、前述したように離れた場所にあるプリンタを利用して印刷したりすることができるという利点も有している。これらの利点を有していることから、近年ネットワーク印刷の利用が爆発的に増えている。
また、公開鍵証明書とこれに対応する秘密鍵とを保有するプリンタが開示され、ドキュメントサーバもしくはユーザクライアントからの要求に応じて公開鍵証明書に基づくプリンタ認証を行う技術が開示されている（例えば、特許文献１を参照）。
【０００４】
【特許文献１】特開２００２－２５９１０８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、ネットワークやインターネットは不特定多数の人間が利用しており、その気になれば前記ネットワークやインターネットに流れている印刷データを第三者が容易に盗み見ることができる。
【０００６】
例えば、有価証券や社外秘情報などの重要なデータをインターネットの先につながっている顧客先で印刷したり、外出先の営業マンが最寄りのプリンタに印刷したりするようなケースでは、印刷データが盗み取られたり、印刷データがプリンタに届くまでに改ざんされたり、プリンタドライバが指定したプリンタと異なるプリンタに印刷データが印刷されてしまったりしては非常に困ることになる。
【０００７】
ところが、従来の技術では、ネットワークやインターネットなどの通信媒体を経由して印刷を行なう際に、印刷データが盗み取られると、前記盗み取られた印刷データが第三者に利用されてしまうという問題点があった。
【０００８】
本発明は前記の問題点に鑑みてなされたもので、ネットワークやインターネットなどの通信媒体を経由して印刷を行なう際に、たとえ印刷データが盗み取られたとしても、前記盗み取られた印刷データが第三者に利用されてしまうことを可及的に防止することができるようにすることが第１の側面である。
また、ネットワークやインターネットなどの通信媒体を経由して印刷を行なう際に、印刷データが盗み取られて改ざんされた場合にはそれを検知して誤った印刷を防止するよう

にすることが第２の側面である。
　また、ネットワークやインターネットを介して画像形成装置管理サーバから画像形成装置の印刷先の好適な一例であるポートやURLやその他の情報を取得する際に、印刷先データ等の情報が盗み取られることを防止することができるようにすることが第３の側面である。
【課題を解決するための手段】
　【０００９】
　本発明の印刷制御装置は、印刷データを含んだ印刷ジョブを、通信媒体を介して指定の画像形成装置に送信して、前記指定の画像形成装置により前記印刷データを印刷するように制御する印刷制御装置であって、前記印刷ジョブの印刷が指定された画像形成装置で復号化することが可能な暗号化方法で前記印刷データを暗号化する印刷データ暗号化手段と、前記画像形成装置に対応する出力先を示す情報を取得する取得手段と、前記取得手段が取得した出力先を示す情報を復号する復号手段とを備えたことを特徴とする。
　【００１０】
　本発明の画像形成装置は、通信媒体を介して受信した印刷ジョブに含まれる暗号化された印刷データを印刷する画像形成装置であって、前記暗号化された印刷データを所定の複号化方法で復号化する印刷データ復号化手段と、前記受信した印刷ジョブから特徴量を取得する特徴量取得手段と、前記印刷データ復号化手段により復号化された印刷データから特徴量を算出する特徴量算出手段と、画像形成装置に対応する出力先を示す情報を暗号化して転送する転送手段と、前記特徴量算出手段により算出された特徴量と、前記特徴量取得手段によって取得された特徴量とを比較し、両者が一致していることを確かめることで、前記暗号化された印刷データに破損や改ざんが無いことを確認する印刷データ確認手段とを有することを特徴とする。
　【００１１】
　本発明の画像形成装置管理サーバは、通信媒体を介して接続された画像形成装置の情報を管理する画像形成装置管理サーバであって、前記通信媒体を介して接続された使用可能な画像形成装置の設置位置や能力、及び各画像形成装置の暗号鍵を含む情報の一覧を所持する情報所持手段と、前記画像形成装置の印刷制御を行なう印刷制御装置からの問合せに応じて、前記情報所持手段により所持されている情報の一覧を参照して、印刷データの印刷を行なうのに適した画像形成装置を選択する画像形成装置選択手段と、前記印刷制御装置からの問合せに応じて、前記画像形成装置選択手段により選択された画像形成装置の暗号鍵やアドレス情報を取得する画像形成装置情報取得手段と、前記印刷制御装置から受信した暗号化された印刷データを、前記情報所持手段により所持されている暗号鍵で復号化し、さらに、前記復号化した印刷データを前記画像形成装置情報取得手段により取得した画像形成装置の暗号鍵で再度暗号化し、前記再度暗号化した印刷データを、前記画像形成装置情報取得手段により取得したアドレスに送信する画像形成装置情報送信手段とを有することを特徴とする。
　【００１２】
　本発明の印刷制御方法は、印刷データを含んだ印刷ジョブを、通信媒体を介して指定の画像形成装置に送信して、前記指定の画像形成装置により前記印刷データを印刷するように制御する印刷制御方法であって、前記印刷ジョブの印刷が指定された画像形成装置で復号化することが可能な暗号化方法で前記印刷データを暗号化する印刷データ暗号化処理を行ない、前記画像形成装置に対応する出力先を示す情報を取得し、取得した出力先を示す情報を復号することを特徴とする。
　【００１３】
　本発明のコンピュータ読み取り可能な記憶媒体は、印刷データを含んだ印刷ジョブを、通信媒体を介して指定の画像形成装置に送信して、前記指定の画像形成装置により前記印刷データを印刷するように制御するに際し、前記印刷ジョブの印刷が指定された画像形成装置で復号化することが可能な暗号化方法で前記印刷データを暗号化する印刷データ暗号化処理と、前記画像形成装置に対応する出力先を示す情報を取得する取得処理と、前記取

得処理で取得した出力先を示す情報を復号する復号処理と、をコンピュータに実行させるコンピュータプログラムを記憶したことを特徴とする。

【発明の効果】

【００１４】

以上説明したように本発明によれば、印刷データを含んだ印刷ジョブを、通信媒体を介して指定の画像形成装置に送信して、前記指定の画像形成装置により前記印刷データを印刷するように制御するに際して、前記印刷ジョブの印刷が指定された画像形成装置で復号化することが可能な暗号化方法で前記印刷データを暗号化するとともに、前記指定された画像形成装置に対応する出力先を示す情報を取得して復号するようにしたので、たとえ印刷データが含まれている印刷ジョブが盗み取られたとしても、前記印刷データが他の画像形成装置で印刷されることを防止することができ、盗み取られた印刷データが第三者に利用されることを防止することができる。

【００１５】

また、本発明の他の特徴によれば、印刷データから算出した特徴量を暗号化してデジタル署名を作成し、前記作成したデジタル署名を前記印刷ジョブに含めて送信するようにしたので、印刷ジョブの送信元の特定と、印刷ジョブに改ざんがないことを保証することができる。したがって、通信媒体経由で印刷データを印刷する場合でも、印刷データが盗み取られて改ざんされた場合にはそれを検知することができる。これにより、誤った印刷を防止することができ、重要な印刷データを安全に印刷することが可能となる。

【００１６】

また、本発明のその他の特徴によれば、通信媒体に接続された画像形成装置を画像形成装置管理サーバで一括管理させるようにしたので、印刷制御装置及びプリンタは、画像形成装置管理サーバのパブリックキーのみを保持すればよく、また、画像形成装置管理サーバは管理している画像形成装置のパブリックキーのみを保持すればよくなり、複数の印刷制御装置と複数の画像形成装置とからなる大規模なシステムにおいてもメンテナンスに要する労力を大幅に削減することが可能となる。

【発明を実施するための最良の形態】

【００１７】

（第１の実施の形態）

以下、添付の図面を参照しながら本発明の印刷制御装置、画像形成装置、画像形成装置管理サーバ、印刷制御方法、及びコンピュータ読み取り可能な記憶媒体の第１の実施の形態について説明を行なう。

【００１８】

図１は、本発明の第１の実施形態を示し、印刷処理システムの構成の一例を示した概念図である。

本実施の形態では、ユーザは印刷制御装置として配設されるホストコンピュータ３０００から印刷指示の操作を行ない、ネットワーク（ＬＡＮ）１００上で共有されているネットワークプリンタ１５００ａや、インターネット２００を介して接続されているインターネットプリンタ１５００ｂに印刷を行なうケースを想定する。プリンタのほかには、画像形成装置の一例として、スキャナ、ファクシミリ、デジタルカメラ、及び、コピー、プリンタ、ファクシミリ、スキャナなどの機能を備えた複合機（マルチファンクションペリフェラル装置）を含む。

【００１９】

図２は、本発明の第１の実施の形態を示し、印刷処理システムの構成の一例を示したブロック図である。

なお、特に断らない限り、ホストコンピュータ３０００とプリンタ１５００（ネットワークプリンタ１５００ａ及びインターネットプリンタ１５００ｂ）とを接続する形態は、ＬＡＮ、ＷＡＮ、公衆回線、及びインターネット等いかなる形態（通信媒体）であっても適用することができる。

【００２０】

図２において、３０００はホストコンピュータであり、ＲＯＭ３のプログラム用ＲＯＭあるいは外部メモリ１１に記憶された文書処理プログラム等に基づいて図形、イメージ、文字、及び表（表計算等を含む）等が混在した文書処理を実行するＣＰＵ１を備え、システムバス４に接続される各デバイス２～８をＣＰＵ１が総括的に制御する構成である。

【００２１】

また、このＲＯＭ３のプログラム用ＲＯＭ３ｂあるいは外部メモリ１１には、ＣＰＵ１の制御プログラムであるオペレーティングシステムプログラム（ＯＳ）等を記憶する。そして、ＲＯＭ３のフォント用ＲＯＭ３ａあるいは外部メモリ１１には前記文書処理の際に使用するフォントデータ等を記憶する。さらに、ＲＯＭ３のデータ用ＲＯＭ３ｃあるいは外部メモリ１１には前記文書処理等を行なう際に使用する各種データを記憶する。

【００２２】

２はＲＡＭで、ＣＰＵ１の主メモリ、ワークエリア等として機能する。

５はキーボードコントローラ（ＫＢＣ）で、キーボード９や不図示のポインティングデバイスからのキー入力を制御する。

６はＣＲＴコントローラ（ＣＲＴＣ）で、ＣＲＴディスプレイ（ＣＲＴ）１０の表示を制御する。

【００２３】

７はディスクコントローラ（ＤＫＣ）で、ブートプログラム、各種のアプリケーション、フォントデータ、ユーザファイル、編集ファイル、及びプリンタ制御コマンド生成プログラム（以下プリンタドライバと称する）等を記憶するハードディスク（ＨＤ）や、フレキシブルディスク（ＦＤ）等の外部メモリ１１とのアクセスを制御する。

【００２４】

８はプリンタコントローラ（ＰＲＴＣ）で、ネットワーク１００を介してプリンタ１５００に接続されて、プリンタ１５００との双方向通信制御処理を実行する。なお、このプリンタコントローラ８は、印刷ジョブをプリンタ１５００に送信する際に、接続プロトコルに応じたコマンドを前記印刷ジョブに付加する場合もある。また、前記コマンドはオペレーティングシステムプログラム（ＯＳ）が自動的に付加する場合もある。

【００２５】

なお、ＣＰＵ１は、例えばＲＡＭ２上に設定された表示情報ＲＡＭへのアウトラインフォントの展開（ラスタライズ）処理を実行し、ＣＲＴ１０上でのウィジウィグ（ＷＹＳＩＷＹＧ）を可能としている。

【００２６】

また、ＣＰＵ１は、ＣＲＴ１０上の不図示のマウスカーソル等で指示されたコマンドに基づいて登録された種々のウインドウを開き、種々のデータ処理を実行する。ユーザは印刷を実行する際に、印刷の設定に関するウインドウを開く。そして、前記開いたウインドウを用いてプリンタの設定や、印刷モードの選択などを含むプリンタドライバに対する印刷処理の設定を行なう。

【００２７】

プリンタ１５００において、１２はプリンタＣＰＵで、ＲＯＭ１４のプログラムＲＯＭに記憶された制御プログラム等、あるいは外部メモリ２１に記憶された制御プログラム等に基づいて、システムバス１５に接続される印刷部インターフェース（印刷部Ｉ／Ｆ）１６を介して印刷部（プリンタエンジン）１７に出力情報としての画像信号を出力する機能を有する。

【００２８】

また、このＲＯＭ１４のプログラムＲＯＭに１４ｂは、ＣＰＵ１２の制御プログラム等を記憶する。また、ＲＯＭ１４のフォント用ＲＯＭ１４ａは、前記出力情報を生成する際に使用するフォントデータ等を記憶する。そして、ＲＯＭ１４のデータ用ＲＯＭ１４ｃは、ハードディスク等の外部メモリ２１がないプリンタの場合に、ホストコンピュータ３０００上で利用される情報等を記憶する。

【００２９】

ＣＰＵ１２は入力部１８を介してホストコンピュータ３０００との通信処理が可能となっており、プリンタ１５００内の情報等をホストコンピュータ３０００に通知することが可能となるように構成されている。

【００３０】

プリンタドライバから受信したデータはＲＡＭ１３に格納され、制御プログラムにより画像信号に変換される。なお、通信プロトコルに応じて付加されているコマンドの解釈も前記制御プログラムにより行なわれる。

【００３１】

ＲＡＭ１３はＣＰＵ１２の主メモリやワークエリア等として機能する記憶媒体であり、図示しない増設ポートに接続されるオプションＲＡＭによりメモリ容量を拡張することができるように構成されている。なお、ＲＡＭ１３は、出力情報展開領域、環境データ格納領域、ＮＶＲＡＭ(不揮発性ＲＡＭ)等に用いられる。

【００３２】

前述したハードディスク（ＨＤ）や、ＩＣカード等の外部メモリ２１は、メモリコントローラ（ＭＣ）２０によりアクセスを制御される。外部メモリ２１は、オプションとして接続され、フォントデータ、エミュレーションプログラム、及びフォームデータ等を記憶する。

【００３３】

また、２２は前述した操作パネルで、操作のためのスイッチやＬＥＤ表示器、液晶パネル等が配設されている。また、前述した外部メモリ２１は１個に限らず、少なくとも１個以上備えているようにしてもよい。そして、内蔵フォントに加えてオプションフォントカードや、言語系の異なるプリンタ制御言語を解釈するプログラムを格納した外部メモリを複数接続することができるように構成されていてもよい。さらに、図示しないＮＶＲＡＭを有し、操作パネル２２からのプリンタモード設定情報を記憶するようにしてもよい。

【００３４】

図３（ａ）に示すのが、本実施の形態のホストコンピュータ３０００のプログラムＲＯＭ３ｂに記憶されている制御プログラムが、ホストコンピュータ３０００上のＲＡＭ２にロードされ実行可能となった状態のメモリマップである。

【００３５】

本実施の形態のホストコンピュータ３０００で使用する暗号化処理(encryption)やデータ特徴量算出関数等は、印刷処理関連プログラム３０４の一部として存在する。また、印刷が指定されたプリンタのパブリックキー（公開鍵）やプリンタドライバ自身のプライベートキー（秘密鍵）は関連データ３０３の一部として存在する。

【００３６】

図３（ｂ）に示すのが、本実施の形態のプリンタ１５００のプログラムＲＯＭ１４ｂに記憶されている制御プログラムが、プリンタ１５００上のＲＡＭ１３にロードされ実行可能となった状態のメモリマップである。

本実施の形態のプリンタ１５００で使用する復号化処理(decryption)やデータ特徴量算出関数等は、印刷処理関連プログラム３１３の一部として存在する。また、特定プリンタドライバのパブリックキーやプリンタ自身のプライベートキーは関連データ３１２の一部として存在する。

【００３７】

図４は、本実施の形態に関わる印刷処理システム（図５以降のフロー図）で用いる暗号鍵を説明する図である。本実施の形態では、暗号法として公開鍵暗号法と共通鍵暗号法を用いており、また、各情報機器でパブリックキーとプライベートキーが存在するため、図４ではそれぞれの鍵を区別して表現している。

また、図４において、データに鍵がオーバライドされている絵は、そのデータが該当する鍵で暗号化されていることを示している。

【００３８】

本実施の形態に関わる印刷処理システムでは、公開鍵暗号法を用いて暗号化した印刷デ

ータを送信することで、指定したプリンタ以外では印刷できない仕組みとなっている。なお公開鍵暗号法とは、自分と相手で違う暗号鍵（プライベートキーとパブリックキー）を用いて暗号化と復号化を行なう方法であり、どちらか一方の鍵で暗号化したデータはもう一方の鍵を使わないと復号化できない。

【００３９】

この公開鍵暗号法(public key structure)では、通常、パブリックキーは公開し、プライベートキーは秘密に保持する。公開鍵暗号法では通信相手ごとに暗号鍵を用意する必要がなく、パブリックキーは公開することができるので相手に暗号鍵を渡すのが非常に楽でありながら、復号化することができるのは自分だけに限定することができる。

【００４０】

この公開鍵暗号法を例えば本実施の形態のプリンタ１５００に適用すると、公開されているプリンタのパブリックキーで印刷データを暗号化しておけば、どのプリンタドライバから印刷データを送信した場合であっても、送信先のプリンタでのみ印刷することが可能であり、他のプリンタでは印刷できないように制限することが可能となる。

【００４１】

以下、図５に示す処理フロー図を用いて、プリンタドライバが暗号化された印刷ジョブを作成する処理を詳しく説明する。

ホストコンピュータ３０００のプリンタドライバは、アプリケーションから印刷要求を受けて印刷データを受け取ると、その印刷データを送信先のプリンタ１５００のパブリックキーで暗号化する（ステップＳ５０１）。

【００４２】

その後、暗号化された印刷データを印刷ジョブとしてプリンタ１５００に送信する。

なお、プリンタ１５００のパブリックキーは公開されており、前記プリンタドライバは出力対象となるプリンタ１５００のパブリックキーを選択して適用する。

【００４３】

以下、図６に示す処理フロー図を用いて、プリンタ１５００が受信した印刷ジョブから印刷データを取得する処理を詳しく説明する。

プリンタ１５００は、受信した印刷ジョブ中の印刷データをプリンタ１５００のプライベートキーで復号化し（ステップＳ６０１）、印刷データを取得する。

【００４４】

なお、前述したように、プリンタ１５００のプライベートキーは、そのプリンタ１５００が非公開で保持している。

ここで指定外のプリンタで印刷データを印刷しようとした場合、前記印刷データは暗号化されているためそのままでは解読も印刷も不可能である。また、暗号を解除する鍵は指定されたプリンタ１５００のみが持つため、他のプリンタでは復号化を行なうこともできない。したがって、本実施の形態に関わる印刷処理システムでは、たとえネットワーク１００上で印刷データを盗み取られたとしても、その印刷データを他のプリンタで印刷されてしまうことを防止することができる。

【００４５】

（第２の実施の形態）

次に、本発明の印刷制御装置、画像形成装置、画像形成装置管理サーバ、印刷制御方法、及びコンピュータ読み取り可能な記憶媒体の第２の実施の形態について説明する。なお、本実施の形態に関わる印刷処理システムのハードウェアの構成は、前述した第１の実施の形態と同様の構成である。したがって、前述した第１の実施の形態と同一部分については図１～図６に示した符号と同一の符号を付し詳細な説明を省略する。

【００４６】

前記第１の実施形態では、たとえ印刷データを盗み取られても他のプリンタへ印刷することを防ぐ印刷処理システムについて説明した。

【００４７】

しかしながら、プリンタ１５００のパブリックキーは公開されている。このため、例え

ば何者かがオリジナルの印刷データをフックして異なる印刷データを、図５に示した処理と同様のステップを経て対象とするプリンタ１５００に流し直した場合などには、プリンタ１５００側でそれが改ざんされた印刷データであるかどうかを判断することができない。このようなことは、例えば印刷データが見積書や有価証券の場合などでは非常に大きな問題になる虞がある。

【００４８】

そこで本実施の形態の印刷処理では、印刷データにデジタル署名をつけたものを印刷ジョブとしてプリンタに送ることで、プリンタ本体で印刷データの改ざんの有無を確認することできるようにする仕組みにしている。

【００４９】

なお、デジタル署名とは、印刷データの内容の特徴量を算出したものをホストコンピュータ３０００のプリンタドライバのプライベートキーで暗号化したものである。プリンタは、特定のプリンタドライバのパブリックキーを内蔵しており、それを用いてデジタル署名を復号化して確認する。

【００５０】

また、前記印刷データの内容の特徴量としては、ハッシュ値やチェックサム等を用いる。ハッシュ値とは、ハッシュ関数から算出される値であり、ハッシュ関数は計算結果から元の値を求めたり、同じハッシュ値になるように改ざんしたりするのが困難な関数である。

【００５１】

以下、図７に示す処理フロー図を用いて、本実施の形態のホストコンピュータ３０００のプリンタドライバが暗号化された印刷ジョブを作成する処理を詳しく説明する。

【００５２】

ホストコンピュータ３０００のプリンタドライバは、アプリケーションから印刷要求を受けて印刷データを受け取ると、その印刷データを送信先のプリンタのパブリックキーで暗号化する（ステップＳ７０１）。

【００５３】

次に、暗号化する前の元の印刷データから特徴量算出関数を通して特徴量を算出し（ステップＳ７０２）、前記特徴量をプリンタドライバのプライベートキーで暗号化する（ステップＳ７０３）。ここで得られたものがデジタル署名となる。その後、ホストコンピュータ３０００は、前記暗号化された印刷データとデジタル署名とを合わせたものを印刷ジョブとして、前記印刷データを印刷するプリンタ１５００に送信する。

【００５４】

以下、図８に示す処理フロー図を用いて、本実施の形態のプリンタ１５００が受信した印刷ジョブから印刷データを取得する処理を詳しく説明する。

【００５５】

プリンタ１５００は、受信した印刷ジョブ中の印刷データをプリンタのプライベートキーで復号化し（ステップＳ８０１）、印刷データを取得する。また、印刷ジョブ中のデジタル署名を、送信元のプリンタドライバのパブリックキーで復号化し（ステップＳ８０２）、前記取得した印刷データの特徴量を取得する。

【００５６】

そして、取得した印刷データから、プリンタ１５００本体でも特徴量取得関数により特徴量を算出し（ステップＳ８０３）、それを受信した印刷データの特徴量と比較し（ステップＳ８０４）、同一値であればステップＳ８０１で取得した印刷データに改ざんがないことが確かめられる。

【００５７】

また、ステップＳ８０４の処理において、プリンタ１５００本体で算出した特徴量と受信した印刷データの特徴量との比較結果が不一致だった場合は次のような状態になることが考えられる。

すなわち、特定のプリンタドライバのパブリックキーで復号化することできず、前記受

信した印刷データの送信元が正規のホストコンピュータと異なる場合と、算出した印刷データの特徴量が前記受信した印刷データの特徴量とが異なり、印刷データに改ざんがある場合とが考えられ、いずれの場合でも印刷ジョブが正しく送信されていないことを検知できる。

【００５８】

このように本実施の形態に関わる印刷処理システムでは、不正な印刷データをプリンタで検出することが可能になる。なお、このように不正な印刷データを検出した場合は、検出後不正な印刷データの出力は行なわず、不正な印刷データを受け取ったことをホストコンピュータに通知するなどの対処を行なうことが可能となる。

【００５９】

なお、本実施の形態では、プリンタ１５００本体でもプリンタドライバと共通の特徴量算出関数を持っている。また、プリンタ１５００本体には、あらかじめ特定のプリンタドライバ（またはホストコンピュータ）のパブリックキーを登録しておくものとする。

【００６０】

なお、プリンタドライバ特有の暗号鍵は、プリンタドライバに特有なものに限らず、ホストコンピュータ３０００に特有なものにしても良いし、使用しているユーザに特有なものにしても良い。

【００６１】

例えば、暗号鍵をホストコンピュータ３０００に特有なものにした場合は、そのホストコンピュータ３００をマルチユーザ形態で利用するようにすれば、そのホストコンピュータ３０００上の誰もが同じ条件で印刷データをプリンタ１５００で印刷することができる。

【００６２】

また、暗号鍵をユーザ特有にした場合は、社内のデスクトップパソコン（ＰＣ）から印刷しても、営業先のノートパソコン（ＰＣ）から印刷しても同じ条件で印刷データを印刷することができる。

【００６３】

このように、暗号鍵をプリンタドライバ特有にした場合、ホストコンピュータ３０００特有にした場合、及びユーザ特有にした場合のいずれの場合であっても、あらかじめプリンタへ登録しておくパブリックキーはひとつで済む。

【００６４】

（第３の実施の形態）

次に、本発明の印刷制御装置、画像形成装置、画像形成装置管理サーバ、印刷制御方法、及びコンピュータ読み取り可能な記憶媒体の第３の実施の形態について説明する。なお、本実施の形態に関わる印刷処理システムのハードウェアの構成は、前述した第１の実施の形態及び第２の実施の形態と同様の構成である。したがって、前述した第１の実施の形態及び第２の実施の形態と同一部分については図１～図８に付した符号と同一の符号を付し詳細な説明を省略する。

【００６５】

前記第１の実施の形態と第２の実施の形態では、印刷データが盗み取られたり、前記盗み取られた印刷データが改ざんされたりすることを防止し、印刷データに対するセキュリティを強化して印刷する場合について説明した。

【００６６】

しかしながら、前述した公開鍵暗号法に基づく印刷データの暗号化及び復号化は、非常に処理時間がかかるため、一般に大きなサイズとなる印刷データに適用するのは好ましくない。

【００６７】

そこで、本実施の形態では、公開鍵暗号法と比べて圧倒的にパフォーマンスの高い（処理時間が短い）共通鍵暗号法を適用した形態について説明する。

【００６８】

ここで、共通鍵暗号法とは、自分と相手が同じ暗号鍵（シークレットキー）を使って暗号化と復号化を行なう方法である。具体的には、文章のビット列を、シークレットキーで示される規則に従って、別のビット列に置き換えたり、シフトしたりすることでデータを暗号化する。

【００６９】

素数同士をかけた値が十分大きい場合に素因数分解することが難しいという性質や、ある値を入力した楕円曲線上の点からその値を推定することが難しいという性質などが利用される公開鍵暗号法の複雑な処理と比べ、共通化暗号法の処理は一般に数百倍速いといわれている。

【００７０】

しかしながら、その一方で、通信相手ごとに安全な方法でシークレットキーを渡す必要があり、また通信相手ごとにシークレットキーを用意する必要がある。

【００７１】

そこで本実施の形態では、公開鍵暗号法と共通鍵暗号法とを組合せ、印刷データはシークレットキーで暗号化し、そのシークレットキーは公開鍵暗号を使ってプリンタに渡すようにしている。

【００７２】

以下、図９に示す処理フロー図を用いて、プリンタドライバが暗号化された印刷ジョブを作成する処理を詳しく説明する。

【００７３】

ホストコンピュータ３０００のプリンタドライバは、アプリケーションから印刷要求を受けて印刷データを受け取ると、まずシークレットキーを作成し（ステップＳ９０１）、作成したシークレットキーで渡された印刷データを暗号化する（ステップＳ９０２）。また作成したシークレットキーは、プリンタ１５００のパブリックキーで暗号化する（ステップＳ９０３）。

【００７４】

次に、暗号化する前の元の印刷データから特徴量算出関数を通して特徴量を算出し（ステップＳ９０４）、前記特徴量をプリンタドライバのプライベートキーで暗号化する（ステップＳ９０５）。ここで得られたものがデジタル署名となる。

【００７５】

その後、ホストコンピュータ３０００は、前記シークレットキーで暗号化された印刷データ、プリンタのパブリックキーで暗号化されたシークレットキー、及びデジタル署名を合わせたものを印刷ジョブとしてプリンタ１５００に送信する。

【００７６】

以下、図１０に示す処理フロー図を用いて、プリンタ１５００が受信した印刷ジョブから印刷データを取得する処理を詳しく説明する。

【００７７】

プリンタ１５００は、受信した印刷ジョブ中のシークレットキーをプリンタのプライベートキーで復号化し（ステップＳ１００１）、前記印刷ジョブ中のシークレットキーを取得する。

【００７８】

次に、前記印刷ジョブ中の印刷データを、前記取得した（復元した）シークレットキーで復号化し（ステップＳ１００２）、印刷データを取得する。

【００７９】

また、前記印刷ジョブ中のデジタル署名を、送信元のプリンタドライバのパブリックキーで復号化し（ステップＳ１００３）、印刷データの特徴量を取得する。

【００８０】

そして、取得した印刷データから、プリンタ本体でも特徴量取得関数により特徴量を算出し（ステップＳ１００４）、算出した特徴量と前記受信した印刷データの特徴量とを比較し（ステップＳ１００５）、各特徴量が同一値であればステップＳ１００２で取得した

印刷データに改ざんがないことが確かめられる。

【００８１】

このように、本実施形態では、時間のかかる公開鍵の暗号化は、シークレットキーの暗号化及び復号化でしか利用せず、ネットワークやインターネットに接続されている複数のプリンタごとにシークレットキーを管理する必要がない。また、ホストコンピュータ３０００は、プリンタと通信するごとにシークレットキーを変更することができるので、プリンタ１５００に送信する印刷データに対する安全性も高くなる。

【００８２】

（第４の実施の形態）

次に、本発明の印刷制御装置、画像形成装置、画像形成装置管理サーバ、印刷制御方法、及びコンピュータ読み取り可能な記憶媒体の第４の実施の形態について説明する。

【００８３】

前述した第１～第３の実施の形態では、指定されたプリンタでのみ復号化することが可能な手段で印刷データを暗号化することで、前記印刷データの横取りを防ぐ手法や、デジタル署名（印刷データの特徴量を送信元が自身のプライベートキーで暗号化したもので、送信元のパブリックキーで復号化して内容を確認することでデータの改ざんを検出できる）を印刷データに付加することで印刷データの改ざんを防ぐ手法などについて説明した。

【００８４】

しかしながら、前述した第１～第３の実施の形態で説明した手法だと、ホストコンピュータ（またはプリンタドライバ）は指定可能なすべてのプリンタのパブリックキーを知っておく必要がある。また同様に、プリンタ本体にもすべてのプリンタドライバのパブリックキーを登録しておかなければならない。

【００８５】

したがって、ホストコンピュータもプリンタも複数利用することが可能な大規模な印刷処理システムでは、それらの情報の登録やメンテナンスには莫大な労力を要する。

【００８６】

そこで、本実施の形態では、前述した第１～第３の実施の形態で説明した印刷処理システムにおけるインターネットやネットワーク上での安全な印刷データ送信の仕組みは踏襲しつつ、その処理で必要なプリンタのパブリックキー等の情報は、画像形成装置管理サーバとして配設されるプリンタ管理サーバが一括管理し、プリンタドライバはプリンタ管理サーバから必要な情報を取得することで個々のプリンタの情報を管理する必要をなくす印刷処理システムについて説明する。

【００８７】

このように、本実施の形態に関わる印刷処理システムにおけるハードウェアの構成は、第１～第３の実施の形態で説明した印刷処理システムにプリンタ管理サーバを付加した構成である。したがって、第１～第３の実施の形態と同一部分には、図１～図３に付した符号と同一の符号を付して詳細な説明を省略する。

【００８８】

図１１は、本発明の第４の実施形態を示し、印刷処理システムの構成の一例を示した概念図である。

ユーザはホストコンピュータ３０００から印刷指示の操作を行ない、ネットワーク（ＬＡＮ）１００上で共有されているネットワークプリンタ１５００ａや、インターネット２００を介して接続されているプリンタ１５００ｂに印刷を行なうケースを想定する。

【００８９】

ここでプリンタ管理サーバ４０００（４０００ａ、４０００ｂ）は、印刷可能なプリンタの情報（設置位置やアドレス、暗号鍵など）を管理しており、ホストコンピュータ３０００は、印刷実行時に前記プリンタ管理サーバ４０００から必要なプリンタの情報を取得して該当するプリンタに印刷データを送信する。

【００９０】

また、本実施の形態に関わる印刷処理システムでは、前記プリンタ管理サーバ４０００

を通して印刷データをプリンタ４０００ａ、４０００ｂに送信することも可能とする。なお、前記プリンタ管理サーバ４０００は、ＬＡＮ１００上に接続されていても良いし、インターネット２００の先に接続されていても良い。

【００９１】

図１２は、本発明の第４の実施の形態を示し、印刷処理システムの構成の一例を示したブロック図である。

なお、特に断らない限り、ホストコンピュータ３０００とプリンタ１５００を接続する形態はＬＡＮ．ＷＡＮ、公衆回線、インターネット等いかなる形態であっても適用できることは言うまでもない。

【００９２】

図１２において、４０００はプリンタ管理サーバで、プログラムＲＯＭ３３または不図示の外部メモリに記録された制御プログラムを実行するＣＰＵ３１と、ＣＰＵ３１の主メモリや、ワークエリア等として機能するＲＡＭ３２とを備え、システムバス３５に接続される各ユニット３２～３３をＣＰＵ３１が総括的に制御する。

【００９３】

また、３４はネットワークインターフェースカート（Ｎ１Ｃ）で、プリンタドライバやプリンタ１５００との双方向通信処理を行なう。

【００９４】

図１３（ａ）に示すのが、本実施の形態のホストコンピュータ３０００のプログラムＲＯＭ３ｂに記憶されている制御プログラムが、ホストコンピュータ３０００上のＲＡＭ２にロードされ実行可能となった状態のメモリマップである。

【００９５】

本実施の形態のホストコンピュータ３０００で使用する暗号化処理やデータ特徴量算出関数等は、印刷処理関連プログラム３０４の一部として存在する。
また、プリンタ管理サーバ4.０００のパブリックキーやプリンタドライバ自身のプライベートキーは関連データ３０３の一部として存在する。

【００９６】

図１３（ｂ）に示すのが、本実施の形態のプリンタ管理サーバ４０００のプログラムＲＯＭ３３（または不図示の外部メモリ）に記録されている制御プログラムが、プリンタ管理サーバ４０００上のＲＡＭ３２にロードされ実行可能となった状態のメモリマップである。

【００９７】

本実施の形態のプリンタ管理サーバ４０００で使用する暗号化／復号化処理、データ特徴量算出関数、及びプリンタ検索処理等は、サーバ処理関連プログラム３１３の一部として存在する。

【００９８】

また、プリンタ管理サーバ４０００が管理するプリンタ情報（各プリンタの設置位置、アドレス、各プリンタのパブリックキー等）は、関連データ３１２の一部として存在する。

【００９９】

図１３（ｃ）に示すのが、本実施の形態のプリンタ１５００のプログラムＲＯＭ１４ｂに記録されている制御プログラムがプリンタ１５００上のＲＡＭ１３にロードされ実行可能となった状態のメモリマップである。

【０１００】

本実施の形態のプリンタ１５００で使用する、復号化処理やデータ特徴量算出関数等は、印刷処理関連プログラム３２３の一部として存在する。また、プリンタ管理サーバ４０００のパブリックキーやプリンタ自身のプライベートキーは関連データ３２２の一部として存在する。

【０１０１】

図１４は、本実施の形態に関わる印刷処理システム（図１５以降のフロー図）で用いる

暗号鍵を説明する図である。本実施の形態では、暗号法として公開鍵暗号法を用いており、各情報機器でパブリックキーとプライベートキーが存在するため、それぞれの鍵を区別して表現している。

また、図１４において、データに鍵がオーバライドされている絵は、そのデータが該当する鍵で暗号化されている状態を示している。

【０１０２】

本実施の形態に関わる印刷処理システムでは、プリンタドライバがプリンタ管理サーバ４０００からプリンタ１５００の情報を安全な方法で取得し、そのプリンタ１５００に公開鍵暗号法で暗号化した印刷データを送信する仕組みを説明する。

【０１０３】

なお、公開鍵暗号法とは、自分と相手で違う暗号鍵（プライベートキーとパブリックキー）を用いて暗号化と復号化を行なう方法であり、どちらか一方の鍵で暗号化したデータはもう一方の鍵を使わないと復号化することができない。

【０１０４】

この公開鍵暗号法では、通常、パブリックキーは公開し、プライベートキーは秘密に保持する。このように公開鍵暗号法では通信相手ごとに暗号鍵を用意する必要がなく、パブリックキーは公開することができるので相手に暗号鍵を渡すのが非常に楽でありながら、復号することができるのは自分だけに限定することができる。

【０１０５】

この公開鍵暗号法を、例えば本実施の形態に関わる印刷処理システムに適用すると、公開されているプリンタのパブリックキーで暗号化した印刷データを送信すれば、どのプリンタドライバから印刷データを送信した場合であっても、送信先のプリンタでのみ印刷することが可能であり、他のプリンタでは印刷できないように制限することが可能となる。

【０１０６】

また、プリンタドライバがプリンタ管理サーバ４０００からプリンタ情報を安全に取得する方法としては、デジタル署名を利用する。

ここで、デジタル署名とは、送信するデータの内容の特徴量を算出したものを送信元のプライベートキーで暗号化したものである。ここではプリンタ情報をプリンタ管理サーバ４０００のプライベートキーで暗号化したものとなる。

【０１０７】

プリンタドライバは、前記プリンタ管理サーバ４０００のパブリックキーを保持しており、前記パブリックキーを用いて前記デジタル署名を復号化し、前記復号化したデジタル署名と別途送信されたプリンタ情報から算出した特徴量とを比較することで、送信元の身元と印刷データ（印刷ジョブ）の改ざんの有無を確認することができる。

【０１０８】

また、前記特徴量としては、ハッシュ値やチェックサム等を用いる。ハッシュ値とは、ハッシュ関数から算出される値で、ハッシュ関数は計算結果から元の値を求めたり、同じハッシュ値になるように改ざんしたりするのが困難な関数である。

【０１０９】

ユーザがアプリケーション上で印刷操作を行なうと、アプリケーションはプリンタドライバに印刷データを渡し、印刷処理を実行する。ここでプリンタドライバは、最初に出力すべきプリンタを決定し、そのアドレスや暗号鍵を取得するために、プリンタ管理サーバ４０００に対してプリンタ情報探索要求データを送信する。

【０１１０】

なお、前記プリンタ情報探索要求データを受信したプリンタ管理サーバ４０００におけるプリンタの選択基準としては、例えば、

「・自分が外出中に、見積書などを最寄りの（例えばコンビニの）プリンタに印刷したい。」、

「・外出している相手先の最寄りのプリンタに印刷をしたい。」、

「・顧客のプリンタに親展印刷をしたい。」

などのケースが考えられる。そこで、印刷を行なうプリンタを決定するために、ユーザは事前に、もしくは対話的（インタラクティブ）に、プリンタ選択のための操作を行なうものとする。

【０１１１】

以下、図１５に示す処理フロー図を用いて、プリンタ管理サーバ４０００がプリンタ情報を取り出し、プリンタドライバに返信する処理を詳しく説明する。

【０１１２】

プリンタ管理サーバ４０００は、プリンタドライバから受信した前記プリンタ情報探索要求データの内容（プリンタの位置、カラー／両面／ステイプルなどのプリンタの必要能力など）に応じて、自身が管理しているプリンタ情報のリストの中から適切なプリンタを選択し、該当するプリンタに関するプリンタ情報を取り出す（ステップＳ５０１）。

【０１１３】

前記プリンタ情報には、プリンタアドレス（ＩＰ，ＳＭＢ，ＵＲＬなど）や、プリンタのパブリックキー等が含まれるものとする。

【０１１４】

なお、プリンタと、ホストコンピュータとがＨＴＴＰの上に実装されたＳＯＡＰ（シンプル・オブジェクト・アクセスプロトコル）を用いてデータの授受を行なう場合、ＵＲＬ（出力先を示す情報）を暗号化することは有用である。

【０１１５】

図２３は、出力先を示す情報の暗号化処理を示す本発明の実施形態の一例を示す図である。

図２３の第１のステップ（１）で、プリンタ情報として、デバイスＩＤやデバイスの機能と共にプリンタのデータの送付先（この場合は、ＵＲＬ）を、ホストコンピュータ２３０１がユーザからの印刷指示を認識すると、ホストコンピュータ２３０１がプリンタ２３００にＨＴＴＰ上に実装されたＳＯＡＰを用いて要求する。

【０１１６】

図２３の第２のステップ（２）と第３のステップ（３）で、プリンタ２０００は、プリンタ情報の取得要求があったホストコンピュータ２３０１に対して、ＵＲＬ２３０４を含むプリンタ情報を送信する。この際、ＵＲＬ２３０４は、ホストコンピュータ２３０１側の公開鍵２３０２で暗号化される。同時に、又は、その直後に、送信したＵＲＬ２３０４に対して外部からＨＴＴＰのポストメソッドが投入されるのを待つ状態となる。

【０１１７】

図２３の第４のステップ（４）で、ホストコンピュータ２３０１は、ＵＲＬ２３０４を自身の秘密鍵２３０３で復号化する。復号化したＵＲＬ２３０４に対して、ホストコンピュータ２３０１は、ＨＴＴＰのポストメソッドを用いて、プリンタ２３００内の所定の記憶領域を示す当該ＵＲＬ２３０４をめがけて、印刷対象となるデータを投入する。ポストメソッドは、ＨＴＴＰ（Hyper text transfer protocol）に規定されている、所定の記憶領域に対してデータを投入するための遠隔的に呼び出し可能な手続き(procedure)である。例えば、ＩＥＴＦ（インターネット・エンジニアリング・タスクフォース）から発行されているドキュメントであるＲＦＣ2616を参照されたい。

【０１１８】

この際、ＵＲＬ２３０４が生データとして流れると安全ではない。なぜなら、上述の第２のステップ（２）で、プリンタ２３００が外部からのポストメソッドを待つ状態となり、外部から無防備になるからである。つまり、ＵＲＬ２３０４が生(Raw data)で流れると、悪意のある破壊者（evil cracker）からの攻撃にさらされる可能性がある。ＵＲＬ２３０４を知った破壊者が、当該ＵＲＬ２３０４を用いて、プリンタ２３００内のＵＲＬ２３０４に対応した記憶領域に対する書き込みなどの破壊行為(cracking)や不法アクセス行為をする可能性がある。そこで、ＵＲＬ２３０４は、プリンタ２３００内でホストコンピュータ２３０１から取得した公開鍵で暗号化して送信するのが望ましい。ホストコンピュータ２３０１は、プリンタ２３００から取得した自己のホストコンピュータ２３０１内のＵ

ＲＬ２３０４を、自己の秘密鍵を用いて復号化し、当該復号化したＵＲＬ２３０４を用いて印刷データを、ＨＴＴＰのポストメソッドを用いて送信することになる。

【０１１９】

なお、ＵＲＬ２３０４は、ＵＲＩ（ユニファイド・リソース・アイデンティファイアー）の一例であることは言うまでもない。好適な一例としてＵＲＬを説明したが、他のIPアドレス、NETBEUIが規定するSMBの識別子などのアドレスなど、他の印刷先を示す識別情報、つまり出力先を示す情報や画像形成用データの投入先を示す情報についても安全性を高める効果を奏する。

【０１２０】

なお、前記ステップＳ５０１のプリンタ探索ステップでは、必ずしも１台のプリンタを選択する必要はない。すなわち、前記ステップＳ５０１のプリンタ探索ステップでは、プリンタ管理サーバ４０００が条件（前記プリンタ情報の探索要求データの内容）によってある程度の数のプリンタに絞り、前記絞ったプリンタに関するプリンタ情報をプリンタドライバに一度返送し、プリンタドライバ側でその中から所望するプリンタを選択するという対話的（インタラクティブ）な処理を行なっても良い。

【０１２１】

さらに、プリンタ管理サーバ４０００は、選択するプリンタの数を絞らずに自身が管理しているすべてのプリンタに関するプリンタ情報をプリンタドライバに送信し、プリンタドライバ側で所望するプリンタを選択する構成にしても良い。

【０１２２】

次に、プリンタ管理サーバ４０００は、前記取り出したプリンタ情報から特徴量算出関数を通して特徴量を算出し（ステップＳ５０２）、前記特徴量をプリンタ管理サーバ４０００のプライベートキーで暗号化する（ステップＳ５０３）。このステップＳ５０３で得られたものがデジタル署名となる。最後に、前記プリンタ情報とデジタル署名とをプリンタドライバに返信する。

【０１２３】

以下、図１６に示す処理フロー図を用いて、プリンタドライバが、暗号化された印刷ジョブをプリンタに送信する処理を詳しく説明する。

【０１２４】

プリンタドライバは、プリンタ管理サーバ４０００から返信されたデジタル署名とプリンタ情報のうち、デジタル署名をプリンタ管理サーバ４０００のパブリックキーで復号化し、特徴量を取得する（ステップＳ６０１）。なお、プリンタドライバは、プリンタ管理サーバ４０００のパブリックキーを保持しているものとする。

【０１２５】

次に、プリンタドライバは、取得したプリンタ情報から、プリンタドライバ側でも特徴量取得関数により特徴量を算出し（ステップＳ６０２）、それを受信した特徴量と比較し（ステップＳ６０３）、同一値であれば取得したプリンタ情報が所望するプリンタ管理サーバ４０００からのものであり、且つ印刷データに改ざんがないことが確かめられる。

【０１２６】

次に、プリンタドライバは、プリンタ情報に含まれるパブリックキーを取り出し（ステップＳ６０４）、アプリケーションから渡された印刷データを前記取り出したパブリックキーで暗号化する（ステップＳ６０５）。最後に、暗号化された印刷データを印刷ジョブとしてプリンタ１５００に送信する。

【０１２７】

以下、図１７に示す処理フロー図を用いて、プリンタが、受信した印刷ジョブから印刷データを取得する処理を詳しく説明する。

【０１２８】

プリンタ１５００は、受信した印刷ジョブ中の印刷データをプリンタ１５００のプライベートキーで復号化し（ステップＳ７０１）、印刷データを取得する。

【０１２９】

以上の図１６及び図１７で示した各ステップにより、指定されたプリンタ以外では印刷データを印刷することができないように印刷ジョブを防御しながら、プリンタドライバからプリンタ１５００に印刷ジョブを送信することが可能となる。

【０１３０】

そして、プリンタドライバでは、プリンタ管理サーバ４０００の暗号鍵さえ知っておけば、出力したいプリンタのアドレスや能力、暗号鍵を独自に管理しなくても安全な方法でプリンタ情報を取得することができる。すなわち、プリンタ管理サーバ４０００さえメンテナンスしておけば、いかなるホストコンピュータからでも容易且つ安全に印刷データの印刷を実行することが可能となる。

【０１３１】

（第５の実施の形態）

次に、本発明の印刷制御装置、画像形成装置、画像形成装置管理サーバ、印刷制御方法、及びコンピュータ読み取り可能な記憶媒体の第５の実施の形態について説明する。なお、本実施の形態に関わる印刷処理システムにおけるハードウェアの構成は前述した第４の実施の形態と同様である。したがって、前述した第４の実施の形態と同一部分については図１１～図１５に示した符号と同一の符号を付し詳細な説明を省略する。

【０１３２】

前述の第４の実施の形態では、プリンタドライバのプリンタ情報取得要求によってやり取りされる情報には、プリンタ管理サーバ４０００のデジタル署名がつくため、データが改ざんされる恐れはないものの、ネットワーク上では誰でもが参照することが可能なため、その後の行動を第三者に掌握される恐れがあった。

【０１３３】

そこで、本実施の形態では、プリンタ管理サーバ４０００が返送するデータも暗号化して情報の機密性を高める仕組みの例を示す。

【０１３４】

なお、前述した第４の実施の形態との差異は、プリンタ管理サーバとプリンタドライバとのやり取りのみであり、プリンタ側で暗号化された印刷データを印刷する処理は図１７の処理と同様である。

【０１３５】

ユーザがアプリケーション上で印刷操作を行なうと、アプリケーションはプリンタドライバに印刷データを渡し、印刷処理を実行する。ここでプリンタドライバは、プリンタ管理サーバ４０００に対してプリンタ情報探索要求データを送信する。このとき、本実施例ではサーバ管理の情報を減らすためにプリンタドライバ自身のパブリックキーも送信する。なお、サーバによって管理対象となるプリンタドライバのパブリックキーが管理される場合はこの送信は不要である。

【０１３６】

以下、図８に示す処理フロー図を用いて、プリンタ管理サーバ４０００がプリンタ情報を取り出し、プリンタドライバに返信する処理を詳しく説明する。

【０１３７】

プリンタ管理サーバ４０００は、プリンタドライバから受信した前記プリンタ情報探索要求データの内容に応じて、管理しているプリンタ情報リストの中から適切なプリンタを検索し、該当するプリンタ情報を取り出す（ステップＳ８０１）。本ステップの処理は前記第４の実施の形態で説明したステップＳ５０１と同様である。

【０１３８】

次に、プリンタ管理サーバ４０００は、前記取り出したプリンタ情報を、受信したプリンタドライバのパブリックキーで暗号化する（ステップＳ８０２）。次に、プリンタ管理サーバ４０００は、元のプリンタ情報から特徴量算出関数を通して特徴量を算出し（ステップＳ８０３）、前記特徴量をプリンタ管理サーバ４０００のプライベートキーで暗号化する（ステップＳ８０４）。

このステップＳ８０４で得られたものがデジタル署名となる。最後に、前記暗号化され

たプリンタ情報とデジタル署名とをプリンタドライバに返信する。

【０１３９】

以下、図１９に示す処理フロー図を用いて、プリンタドライバが、暗号化された印刷ジョブをプリンタに送信する処理を詳しく説明する。

【０１４０】

プリンタドライバは、プリンタ管理サーバ４０００から受信したプリンタ情報をプリンタドライバのプライベートキーで復号化し（ステップＳ９０１）、プリンタ情報を取得する。

【０１４１】

また、プリンタドライバは、プリンタ管理サーバ４０００から受信したデジタル署名をプリンタ管理サーバ４０００のパブリックキーで復号化し、プリンタ情報の特徴量を取得する（ステップＳ９０２）。なお、プリンタドライバは、プリンタ管理サーバ４０００のパブリックキーを保持しているものとする。

【０１４２】

次に、プリンタドライバは、取得したプリンタ情報から、プリンタドライバでも特徴量取得関数により特徴量を算出し（ステップＳ９０３）、それを受信した特徴量と比較し（ステップＳ９０４）、同一値であれば取得したプリンタ情報が所望するプリンタ管理サーバ４０００からのものであり、且つ印刷データに改ざんがないことが確かめられる。

【０１４３】

次に、プリンタドライバは、プリンタ情報に含まれるパブリックキーを取り出し（ステップＳ９０５）、アプリケーションから渡された印刷データを前記取り出したパブリックキーで暗号化する（ステップＳ９０６）。最後に、暗号化された印刷データを印刷ジョブとしてプリンタ１５００に送信する。

【０１４４】

以上のステップにより、プリンタ管理サーバ４０００から返信されるプリンタ情報は、プリンタ管理サーバ４０００に要求を発したプリンタドライバでしか見ることができないため、情報機密性を高めることができる。

【０１４５】

また、プリンタドライバは自身のパブリックキーも送っているため、プリンタ管理サーバ４０００は対応すべきプリンタドライバを管理する必要はない。パブリックキーは公開しているものなので、プリンタ管理サーバ４０００に渡すことには問題はない。

【０１４６】

なお、本実施の形態では、プリンタ情報を暗号化する例のみを示したが、プリンタドライバからプリンタ管理サーバ４０００にプリンタドライバ自身のパブリックキーを送信し、それを用いて暗号化した情報をプリンタドライバに返す手段は、他のデータにおいても適用可能である。

【０１４７】

したがって、プリンタ情報以外の他のデータを暗号化する場合であっても、プリンタ管理サーバ４０００がプリンタドライバを管理しなくてもよい仕組みを提供することが可能となる。

【０１４８】

また、本実施の形態では、プリンタドライバの暗号鍵を使用する場合を例に挙げて説明したが、使用する暗号鍵はプリンタドライバのものに限らず、ホストコンピュータ３０００を対象としても良いし、使用しているユーザを対象としても良いことは言うまでもない。

【０１４９】

例えばホストコンピュータ３０００を対象にした場合は、そのホストコンピュータ３０００をマルチユーザ形態で利用するようにすれば、そのホストコンピュータ３０００上の誰もが同じ条件で印刷データをプリンタ１５００で印刷することができる。

【０１５０】

また、ユーザを対象にした場合は、社内のデスクトップパソコン（ＰＣ）から印刷しても営業先のノートパソコン（ＰＣ）から印刷しても同じ条件で印刷データを印刷することができる。

【０１５１】

（第６の実施の形態）

次に、本発明の印刷制御装置、画像形成装置、画像形成装置管理サーバ、印刷制御方法、及びコンピュータ読み取り可能な記憶媒体の第６の実施の形態について説明する。なお、本実施の形態に関わる印刷処理システムにおけるハードウェアの構成は前述した第４の実施の形態及び第５の実施の形態と同様である。したがって、前述した第４の実施の形態及び第５の実施の形態と同一部分については図１１～図１９に示した符号と同一の符号を付し詳細な説明を省略する。

【０１５２】

前述の第４の実施の形態及び第５の実施の形態では、印刷データを指定したプリンタ以外では印刷することができない仕組みを示してきた。

しかしながら、例えば何者かがオリジナルの印刷データをフックして異なる印刷データを、前述した第４の実施の形態及び第５の実施の形態と同様のステップを経て対象とするプリンタに流し直した場合などでは、前記流された印刷データが改ざんされた印刷データであるかどうかをプリンタ側で判断することができない。

【０１５３】

この問題は、印刷データにデジタル署名をつけることで解決を図ることができる。しかし、そのためには、プリンタに対象とするプリンタドライバのパブリックキーを登録しておく必要がある。

【０１５４】

また、印刷処理システム中の全プリンタにパブリックキーを登録しなければならない。さらに、対象とするホストコンピュータが増えたときには、全プリンタをメンテナンスしたりしなければならない。したがって、このような方法で印刷データが改ざんされているか否かを判断すると、非常に大きな労力を要する。

【０１５５】

そこで、本実施の形態では、プリンタ管理サーバ４０００を経由して印刷データを送ることで、印刷データの改ざん防止を図りながらも、プリンタ１５００のメンテナンスをほぼ不要とする仕組みについて説明する。

【０１５６】

以下、図２０に示す処理フロー図を用いて、プリンタドライバがプリンタ管理サーバに印刷データを送信する処理を詳しく説明する。

【０１５７】

ユーザがアプリケーション上で印刷操作を行なうと、アプリケーションはプリンタドライバに印刷データを渡し、印刷処理を実行する。

【０１５８】

ここでプリンタドライバは、まず出力すべきプリンタを決めるために、プリンタ管理サーバ４０００への要求データを作成し、もしくはプリンタ管理サーバ４０００との対話的（インタラクティブ）なやり取りを通してプリンタを特定し（ステップＳ１００１）、プリンタ管理サーバ４０００に送信するプリンタ指定要求を作成する。

【０１５９】

次に、プリンタドライバは、アプリケーションから渡された印刷データをプリンタ管理サーバ４０００のパブリックキーで暗号化する（ステップＳ１００２）。最後に、暗号化された印刷データとプリンタ指定要求をプリンタ管理サーバ４０００に送信する。

【０１６０】

以下、図２１に示す処理フロー図を用いて、プリンタ管理サーバ４０００が暗号化された印刷ジョブをプリンタ１５００に送信する処理を詳しく説明する。

【０１６１】

プリンタ管理サーバ４０００は、プリンタドライバから受信した前記プリンタ指定要求に応じて、管理しているプリンタ情報リストの中から適切なプリンタを選択し、該当するプリンタ情報を取り出す（ステップＳ１１０１）。このプリンタ情報には、プリンタアドレスやプリンタのパブリックキー等が含まれるものとする。

【０１６２】

次に、プリンタ管理サーバ４０００は、プリンタドライバから受信した印刷データを、プリンタ管理サーバ４０００のプライベートキーで復号化し（ステップＳ１１０２）、印刷データを取得する。このステップにより、プリンタ管理サーバ４０００以外の情報機器では印刷データを盗み取ることはできない。

【０１６３】

次に、プリンタ管理サーバ４０００は、前記取得した印刷データを、プリンタ情報の中に含まれるプリンタのパブリックキーで暗号化する（ステップＳ１１０３）。

【０１６４】

次に、プリンタ管理サーバ４０００は、前記取得した印刷データから特徴量算出関数を通して特徴量を算出し（ステップＳ１１０４）、前記算出した特徴量をプリンタ管理サーバ４０００のプライベートキーで暗号化する（ステップＳ１１０５）。ここで得られたものがデジタル署名となる。

【０１６５】

最後に、プリンタ管理サーバ４０００は、前記暗号化された印刷データとデジタル署名とを合わせたものを印刷ジョブとして、前記プリンタ情報に含まれるプリンタアドレスに転送する。

【０１６６】

以下、図２２に示す処理フロー図を用いて、プリンタ１５００が、受信した印刷ジョブから印刷データを取得する処理を詳しく説明する。

【０１６７】

プリンタ１５００は、受信した印刷ジョブ中の印刷データをプリンタ１５００のプライベートキーで復号化し（ステップＳ１２０１）、印刷データを取得する。このステップにより、指定したプリンタ以外の情報機器では印刷データを盗み取ることはできない。

【０１６８】

次に、プリンタ１５００は、受信した印刷ジョブ中のデジタル署名を、送信元のプリンタ管理サーバ４０００のパブリックキーで復号化し（ステップＳ１２０２）、印刷データの特徴量を取得する。

【０１６９】

次に、プリンタ１５００は、前記取得した印刷データから、プリンタ本体でも特徴量取得関数により特徴量を算出し（ステップＳ１２０３）、それを受信した特徴量と比較し（ステップＳ１２０４）、同一値であれば前記ステップＳ１２０１で取得した印刷データに改ざんがないことが確かめられる。

【０１７０】

以上のように本実施の形態では、印刷データが盗み取られてしまうことを防止するほかに、印刷データの改ざんを防止することができる。

また、各情報機器が保持しなければならない他の情報機器のパブリックキーは、プリンタドライバ及びプリンタについてはプリンタ管理サーバ４０００のパブリッタキーのみでよく、また、プリンタ管理サーバ４０００については自身が管理しているプリンタのパブリックキーのみでよい。したがって、印刷処理システムの構成が変わってもメンテナンスが必要なのはプリンタ管理サーバ４０００のみで済む。

【０１７１】

（本発明の他の実施形態）

上述した実施形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、前記実施形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置の

コンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って前記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【０１７２】

また、この場合、前記ソフトウェアのプログラムコード自体が上述した実施形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えば、かかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【０１７３】

また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施形態に含まれることは言うまでもない。

【０１７４】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行ない行ない、その処理によって上述した実施形態の機能が実現される場合にも本発明に含まれることは言うまでもない。

【０１７５】

以上説明した本発明の各実施形態における主要な効果を以下に列挙する。

まず、印刷データを含んだ印刷ジョブを、通信媒体を介して指定のプリンタに送信して、前記指定のプリンタにより前記印刷データを印刷するように制御するに際して、前記印刷ジョブの印刷を指定されたプリンタでのみ復号化することが可能な暗号化方法で前記印刷データを暗号化するようにしたので、たとえ印刷データが含まれている印刷ジョブが盗み取られたとしても、前記印刷データが他のプリンタで印刷されることを防止することができ、盗み取られた印刷データが第三者に利用されることを防止することができる。

【０１７６】

また、印刷データから算出した特徴量を暗号化してデジタル署名を作成し、前記作成したデジタル署名を前記印刷ジョブに含めて送信するようにしたので、印刷ジョブの送信元の特定と、印刷ジョブに改ざんがないことを保証することができる。したがって、通信媒体経由で印刷データを印刷する場合でも、印刷データが盗み取られて改ざんされた場合にはそれを検知することができる。これにより、誤った印刷を防止することができ、重要な印刷データを安全に印刷することが可能となる。

【０１７７】

また、通信媒体に接続されたプリンタをプリンタ管理サーバで一括管理させるようにしたので、印刷制御装置及びプリンタはプリンタ管理サーバのパブリックキーのみを保持すればよく、また、プリンタ管理サーバは管理しているプリンタのパブリックキーのみを保持すればよくなり、複数の印刷制御装置と複数のプリンタとからなる大規模なシステムにおいてもメンテナンスに要する労力を大幅に削減することが可能となる。

【図面の簡単な説明】

【０１７８】

【図１】本発明の第１の実施形態を示し、印刷処理システムの構成の一例を示した概念図である。

【図２】本発明の第１の実施の形態を示し、印刷処理システムの構成の一例を示したブロック図である。

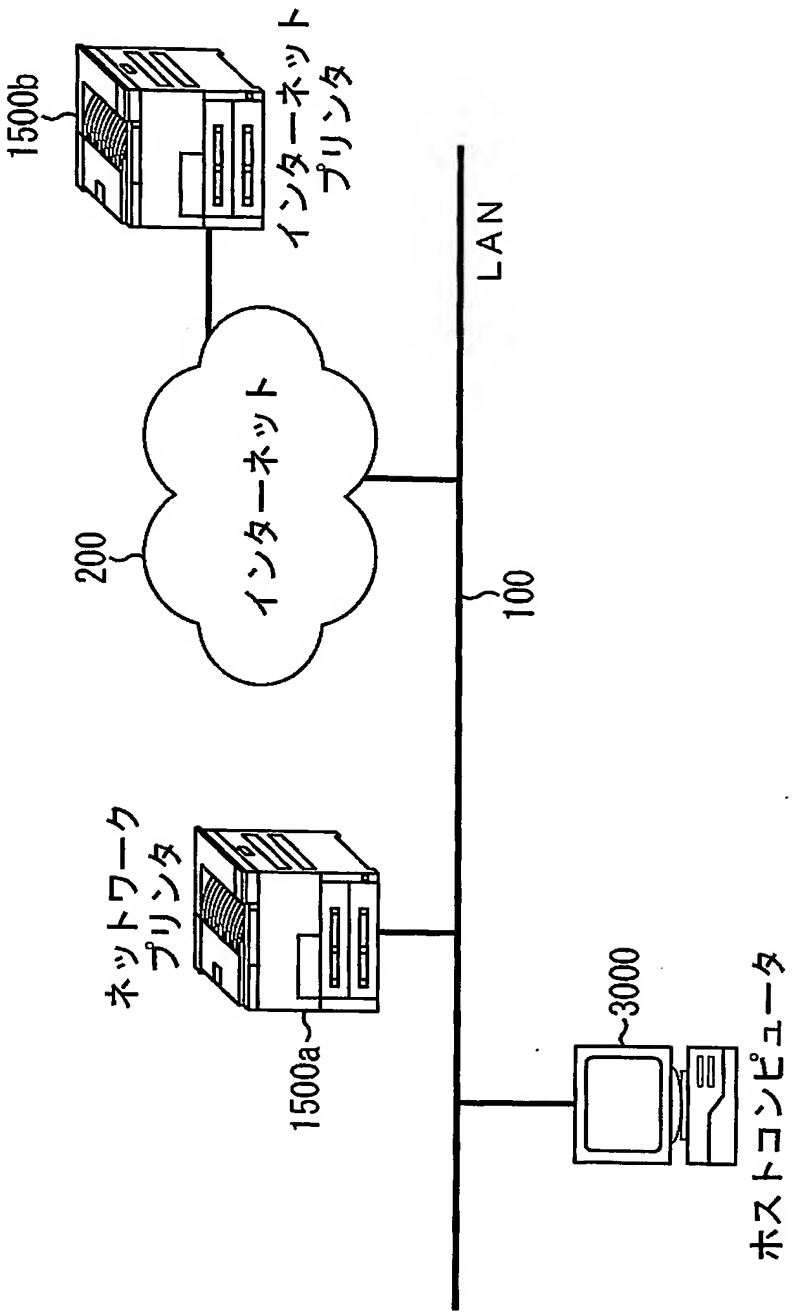
【図３】本発明の第１の実施の形態を示し、ＲＡＭのメモリマップを示す図である。

【図４】本発明の第１の実施の形態を示し、印刷処理システムで用いる暗号鍵を説明

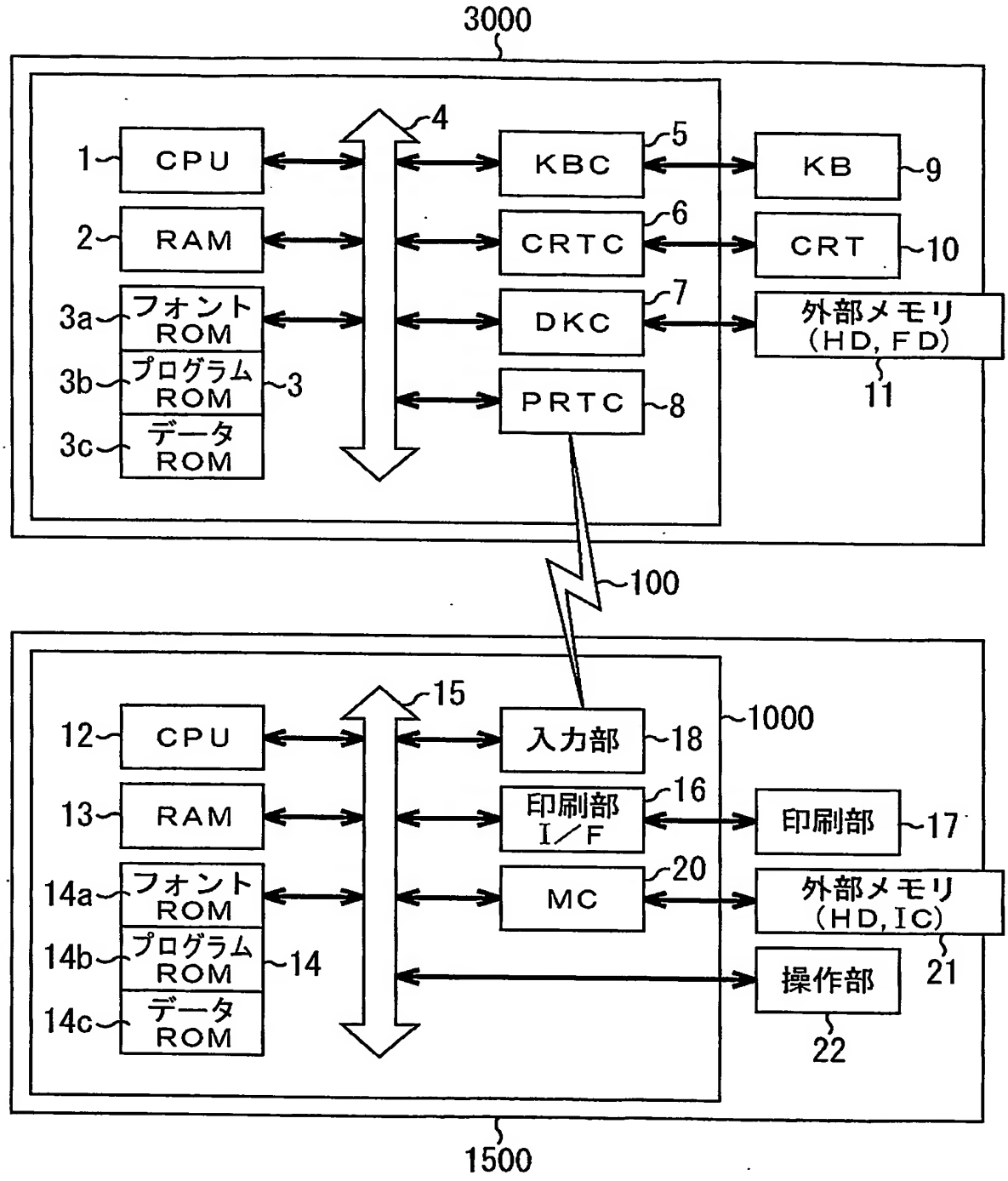
する図である。
【図５】本発明の第１の実施の形態を示し、プリンタドライバの処理を示すフロー図である。
【図６】本発明の第１の実施の形態を示し、プリンタの処理を示すフロー図である。
【図７】本発明の第２の実施の形態を示し、プリンタドライバの処理を示すフロー図である。
【図８】本発明の第２の実施の形態を示し、プリンタの処理を示すフロー図である。
【図９】本発明の第３の実施の形態を示し、プリンタドライバの処理を示すフロー図である。
【図１０】本発明の第３の実施の形態を示し、プリンタの処理を示すフロー図である。
【図１１】本発明の第４の実施形態を示し、印刷処理システムの構成の一例を示した概念図である。
【図１２】本発明の第４の実施の形態を示し、印刷処理システムの構成の一例を示したブロック図である。
【図１３】本発明の第４の実施の形態を示し、ＲＡＭのメモリマップを示す図である。
【図１４】本発明の第４の実施の形態を示し、印刷処理システムで用いる暗号鍵を説明する図である
【図１５】本発明の第４の実施の形態を示し、プリンタ管理サーバの処理を示すフロー図である。
【図１６】本発明の第４の実施の形態を示し、プリンタドライバの処理を示すフロー図である。
【図１７】本発明の第４の実施の形態を示し、プリンタの処理を示すフロー図である。
【図１８】本発明の第５の実施の形態を示し、プリンタ管理サーバの処理を示すフロー図である。
【図１９】本発明の第５の実施の形態を示し、プリンタドライバの処理を示すフロー図である。
【図２０】本発明の第６の実施の形態を示し、プリンタドライバの処理を示すフロー図である。
【図２１】本発明の第６の実施の形態を示し、プリンタ管理サーバの処理を示すフロー図である。
【図２２】本発明の第６の実施の形態を示し、プリンタの処理を示すフロー図である。
【図２３】本発明の実施の形態を示し、出力先を示す情報の暗号化処理の一例を示す図である。

【符号の説明】
【０１７９】
１００　ＬＡＮ
２００　インターネット
１５００　プリンタ
３０００　ホストコンピュータ
４０００　プリンタ管理サーバ

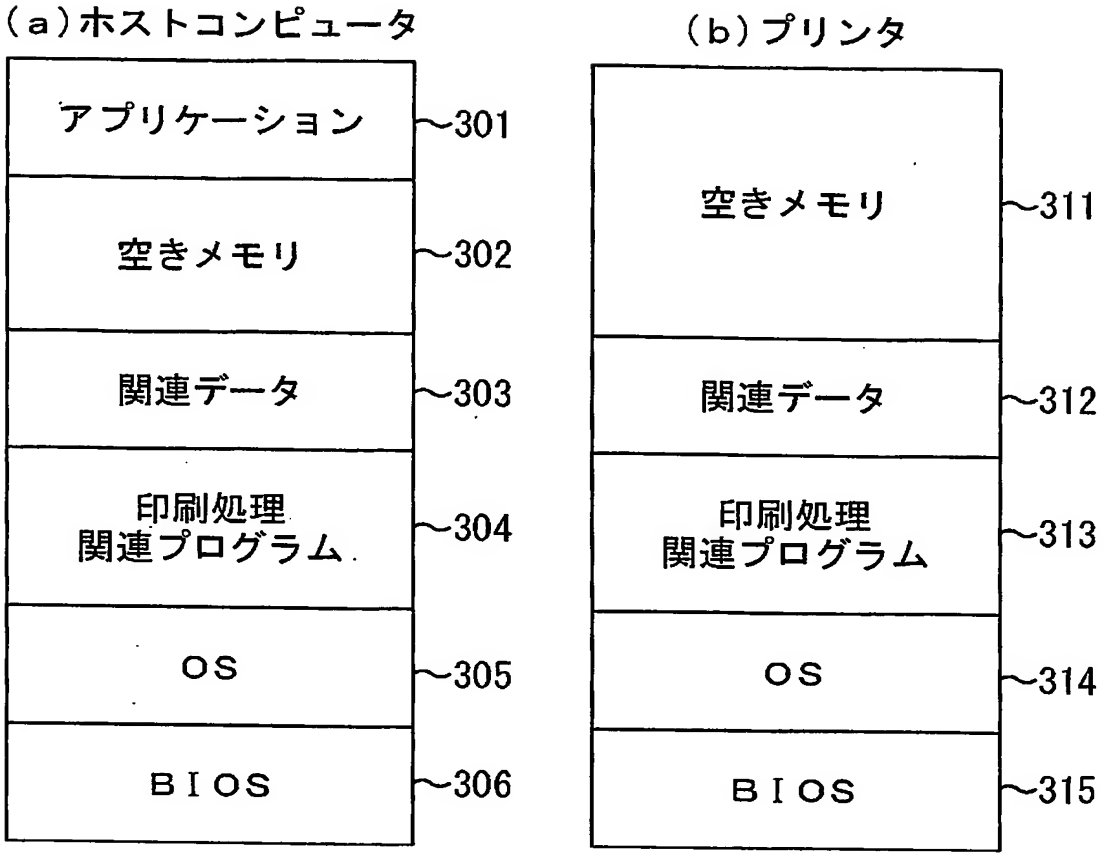
【書類名】図面
【図１】


1500b
インターネット
プリンタ
LAN
インターネット
200
100
ネットワーク
プリンタ
1500a
3000
ホストコンピュータ

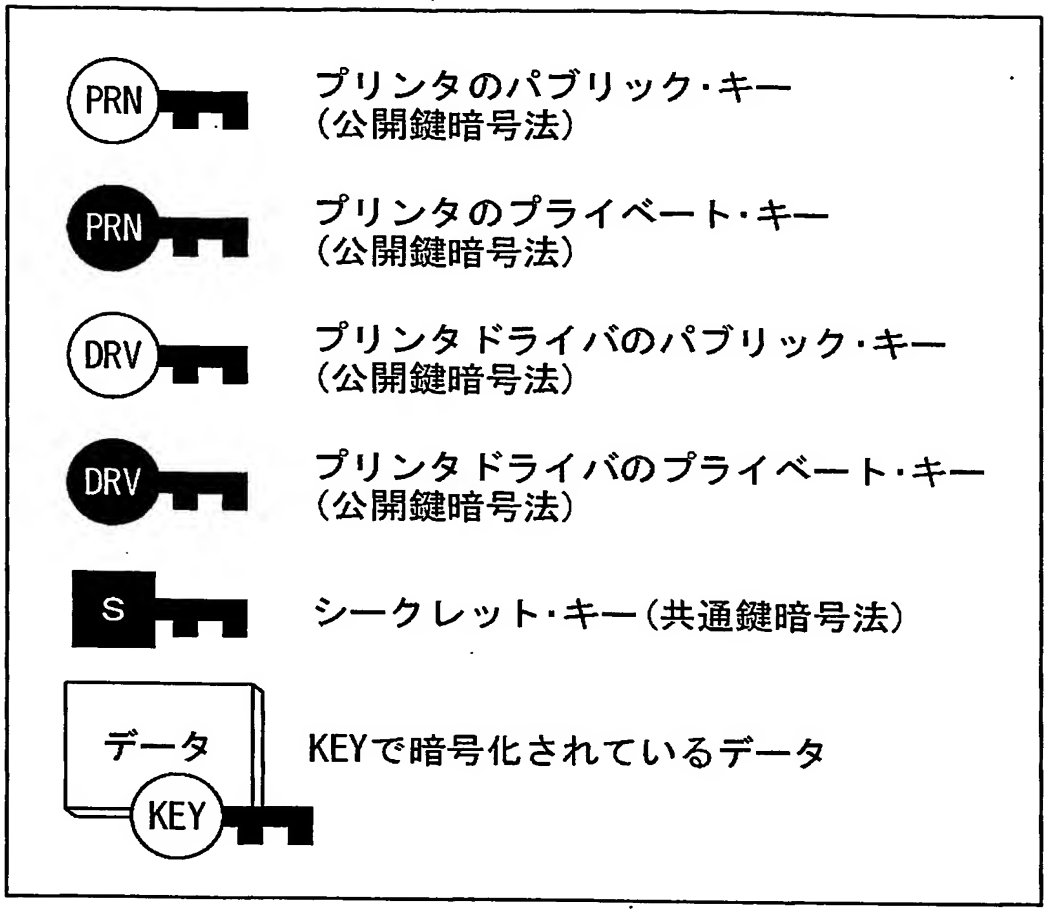
【図２】


3000
1
CPU
2
RAM
3a
フォント ROM
3b
プログラム ROM
3c
データ ROM
3
4
KBC
5
CRTC
6
DKC
7
PRTC
8
KB
9
CRT
10
外部メモリ (HD, FD)
11
100
12
CPU
13
RAM
14a
フォント ROM
14b
プログラム ROM
14c
データ ROM
14
15
入力部
18
印刷部 I／F
16
MC
20
1000
印刷部
17
外部メモリ (HD, IC)
21
操作部
22
1500

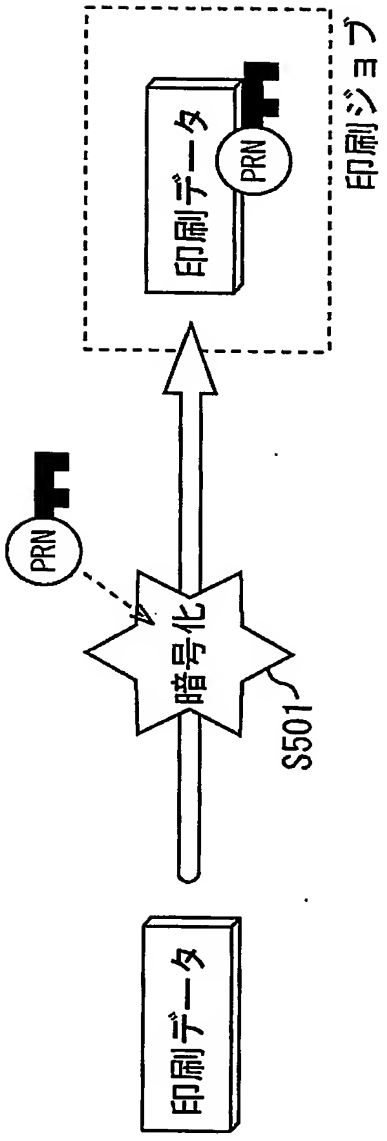
【図３】


(a)ホストコンピュータ
アプリケーション
301
空きメモリ
302
関連データ
303
印刷処理
関連プログラム
304
OS
305
BIOS
306
(b)プリンタ
空きメモリ
311
関連データ
312
印刷処理
関連プログラム
313
OS
314
BIOS
315

【図４】

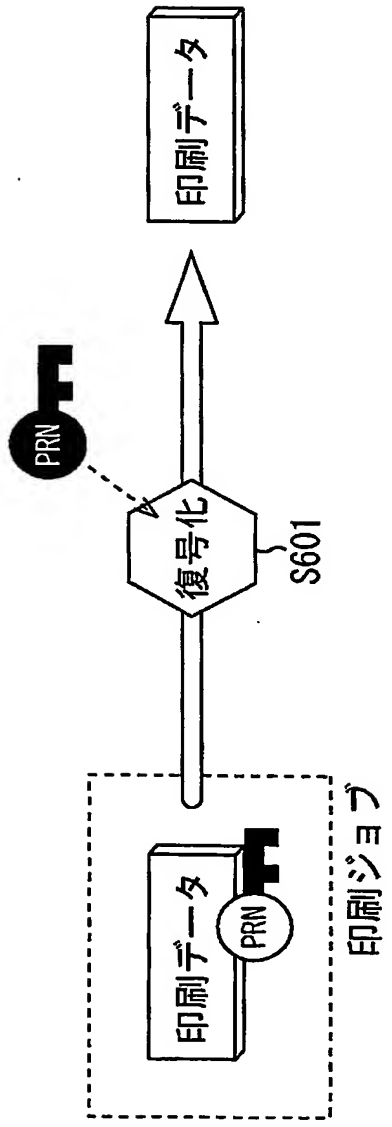

PRN
プリンタのパブリック・キー
(公開鍵暗号法)
PRN
プリンタのプライベート・キー
(公開鍵暗号法)
DRV
プリンタドライバのパブリック・キー
(公開鍵暗号法)
DRV
プリンタドライバのプライベート・キー
(公開鍵暗号法)
S
シークレット・キー(共通鍵暗号法)
データ
KEY
KEYで暗号化されているデータ

【図５】

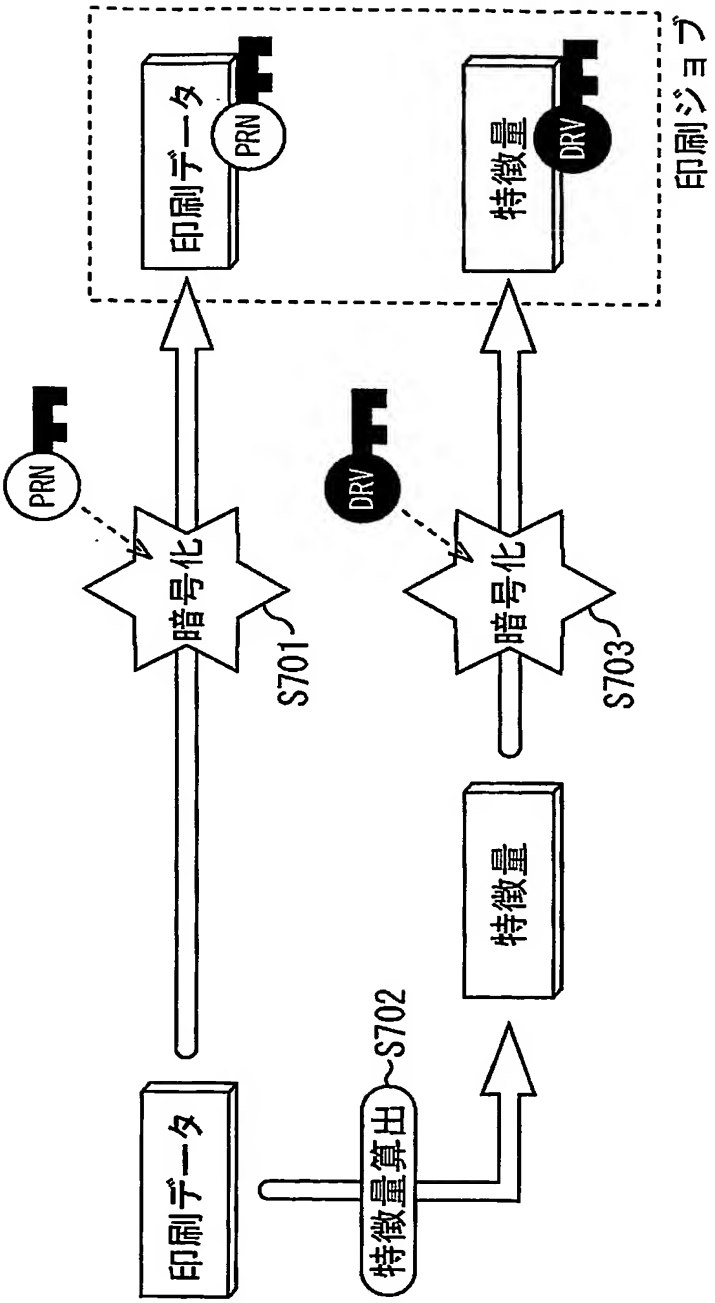


プリンタドライバの処理

【図６】

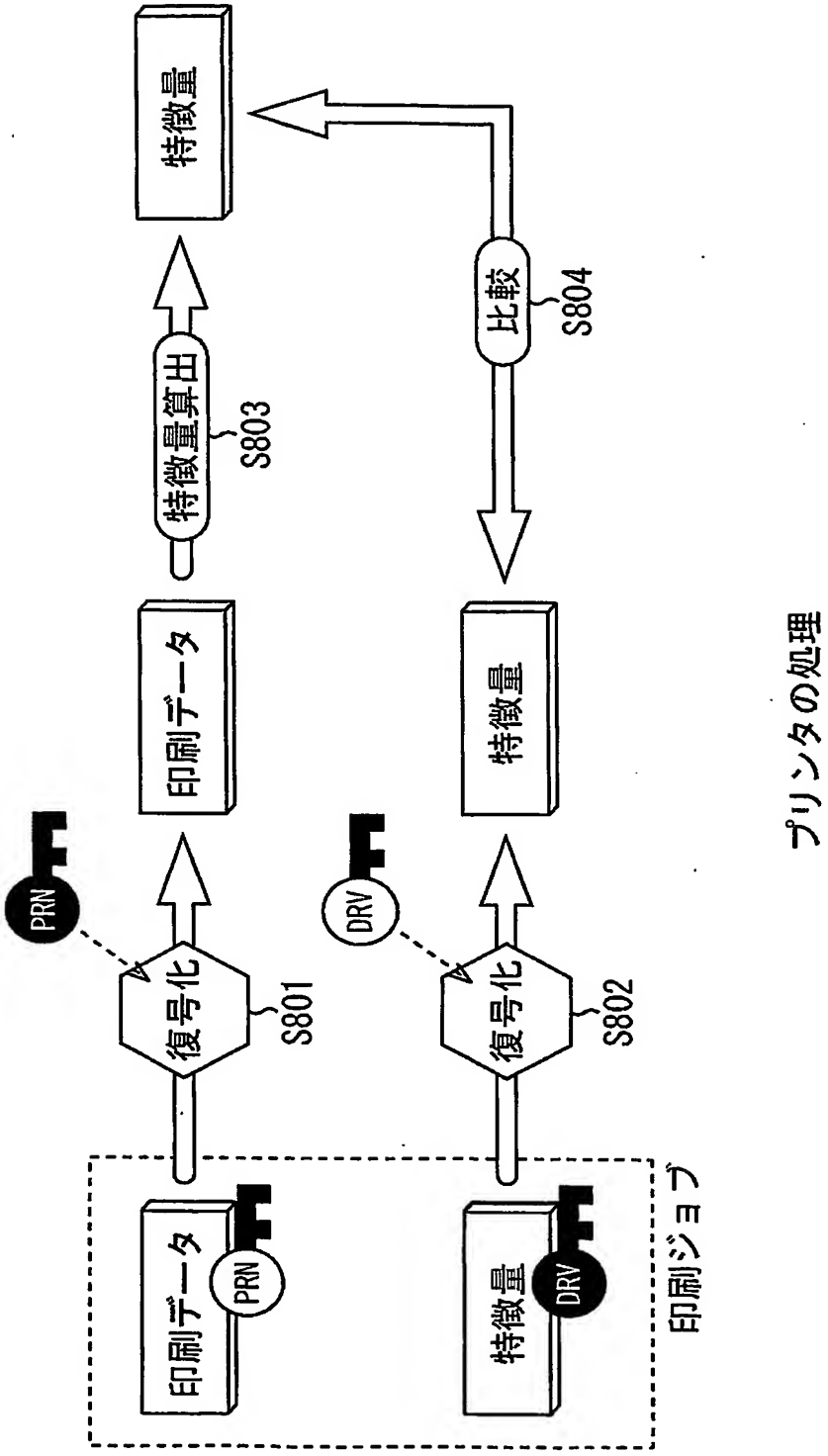


【図７】

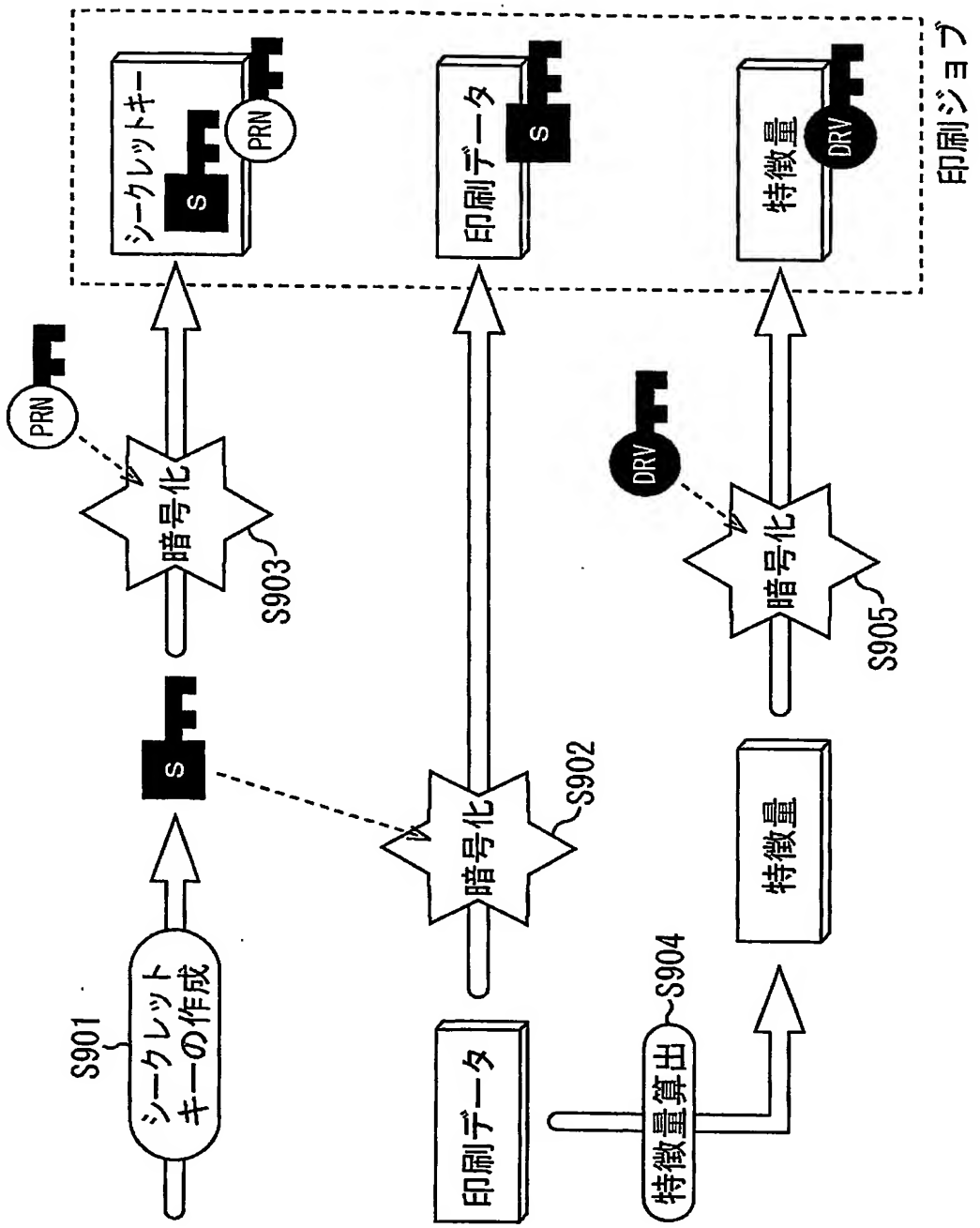


プリンタドライバの処理

【図８】

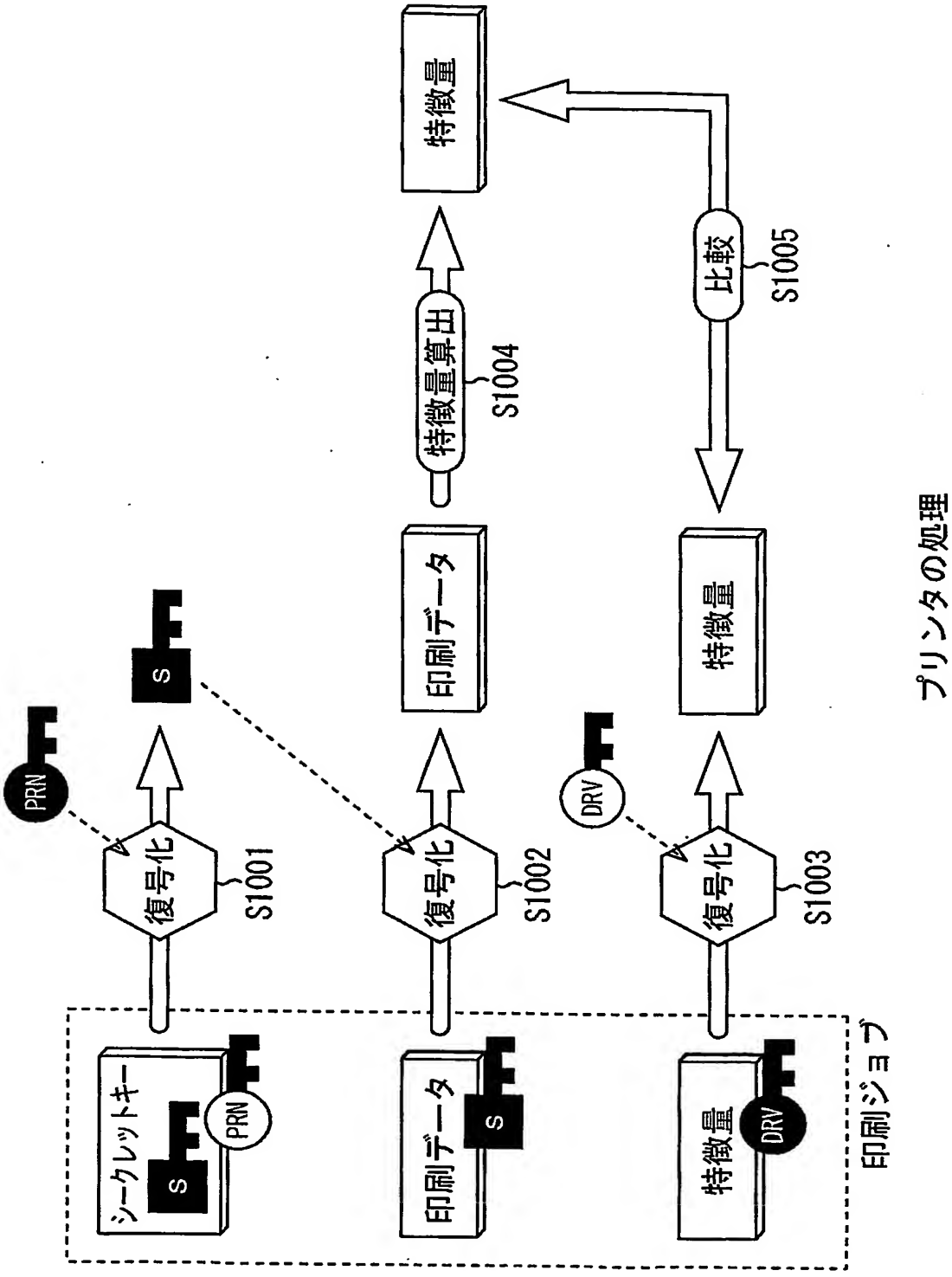

印刷ジョブ
印刷データ
PRN
特徴量
DRV
復号化
S801
復号化
S802
印刷データ
特徴量
特徴量算出
S803
比較
S804
特徴量
プリンタの処理

【図９】

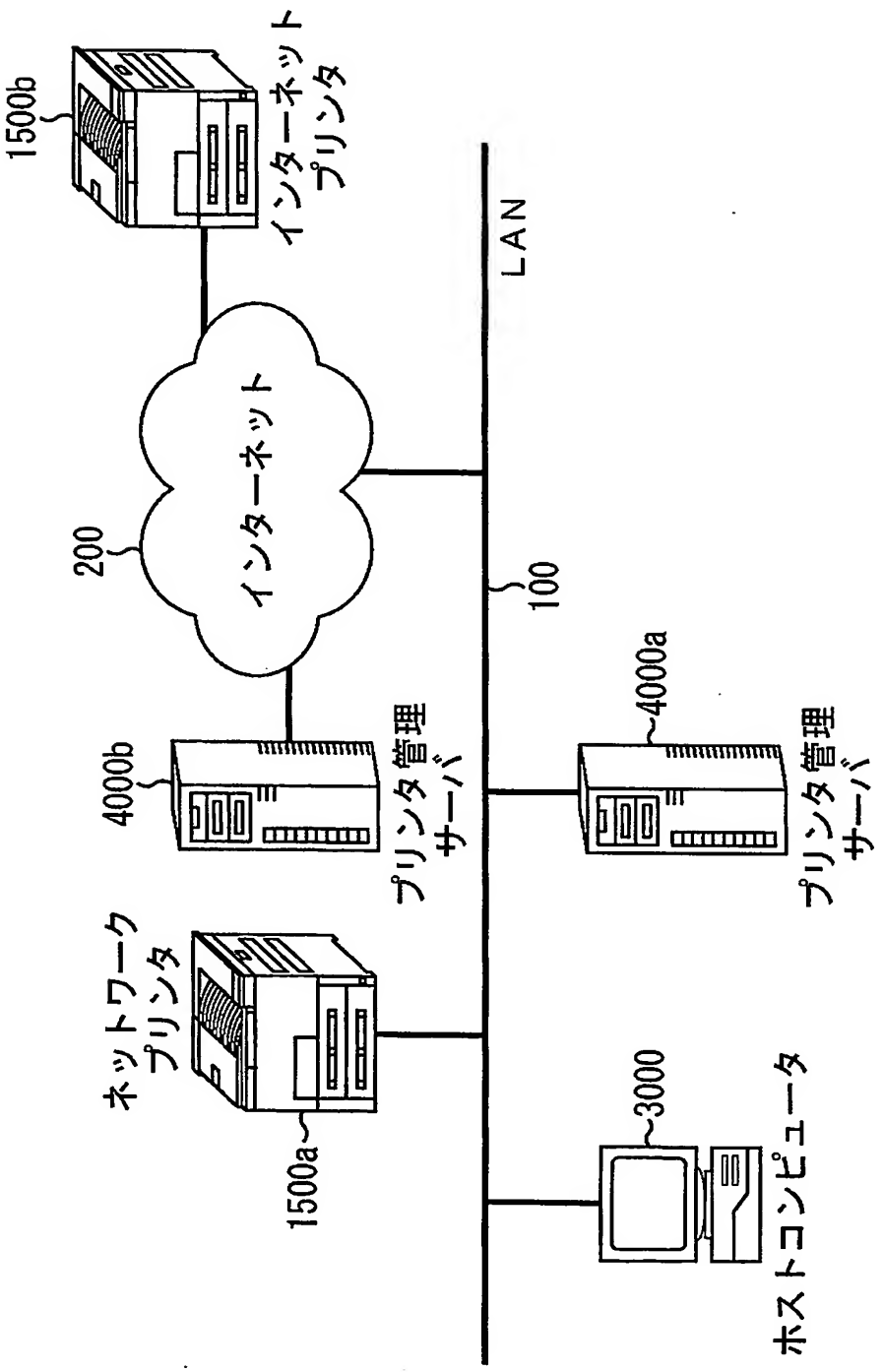


プリンタドライバの処理

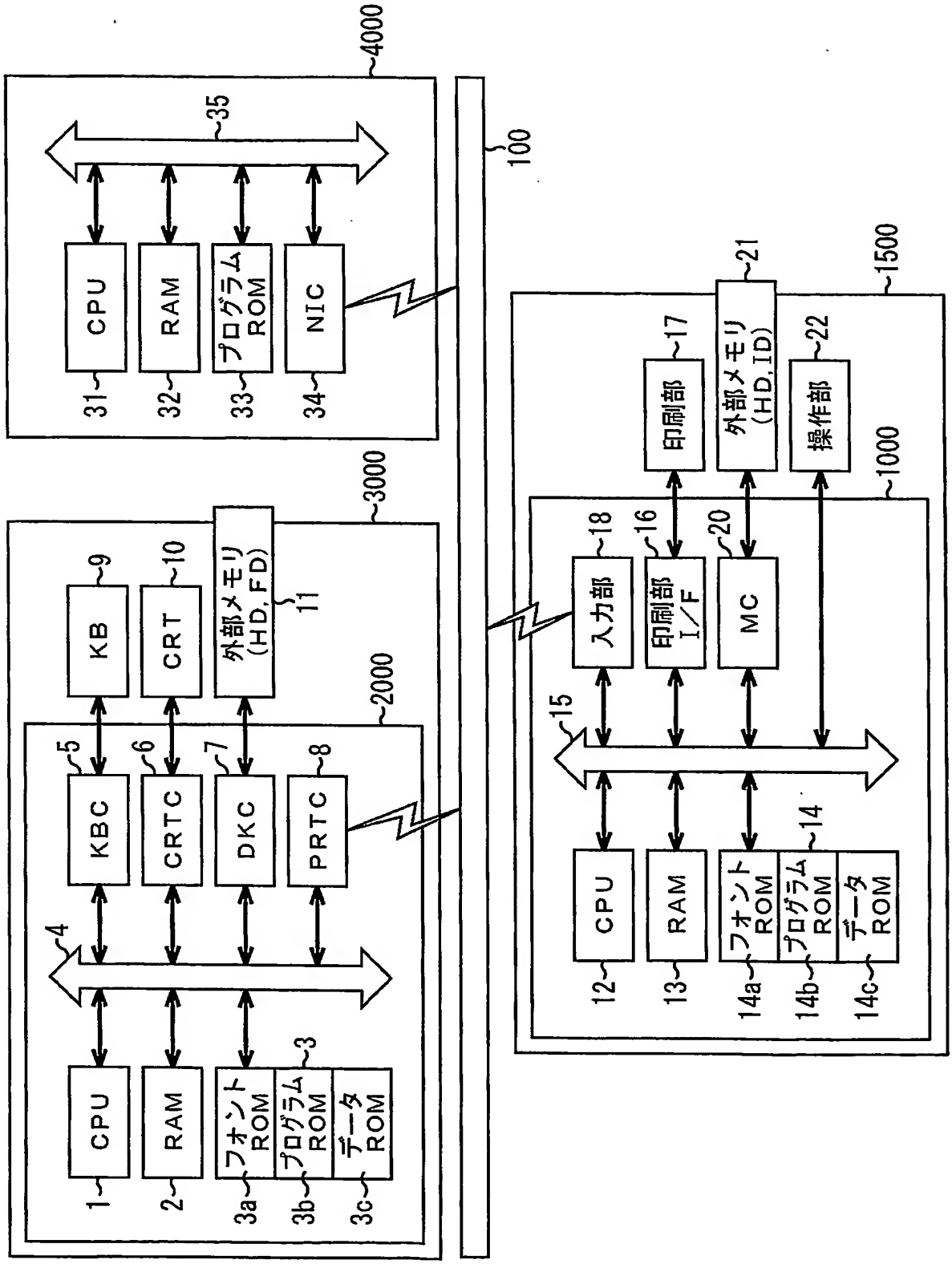
【図１０】


プリンタの処理
印刷ジョブ
シークレットキー
S
PRN
印刷データ
S
特徴量
DRV
復号化
S1001
復号化
S1002
復号化
S1003
PRN
DRV
S
印刷データ
特徴量算出
S1004
特徴量
比較
S1005
特徴量

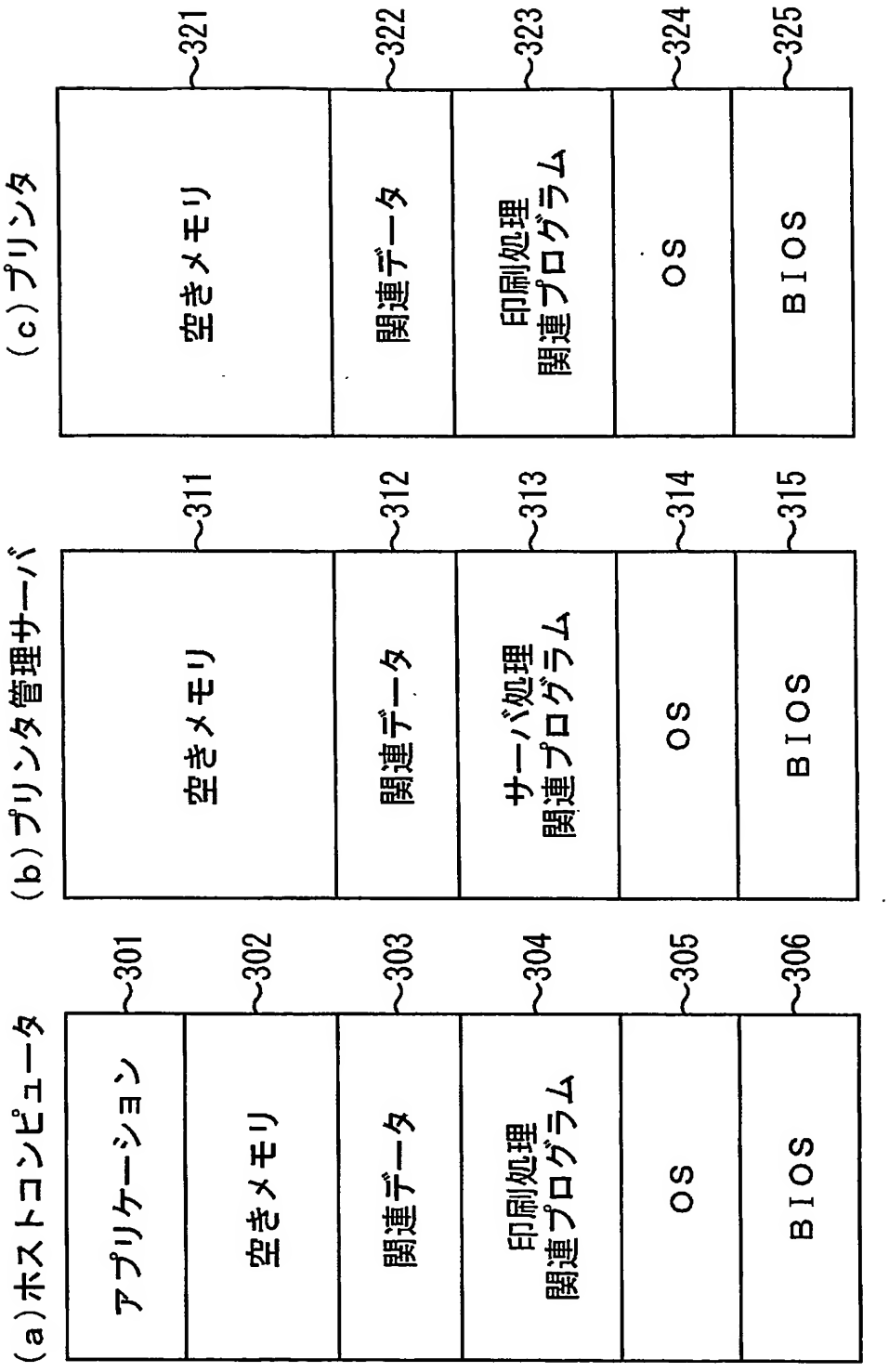
【図１１】


1500b
インターネット
プリンタ
LAN
200
インターネット
100
4000b
プリンタ管理
サーバ
4000a
プリンタ管理
サーバ
ネットワーク
プリンタ
1500a
3000
ホストコンピュータ

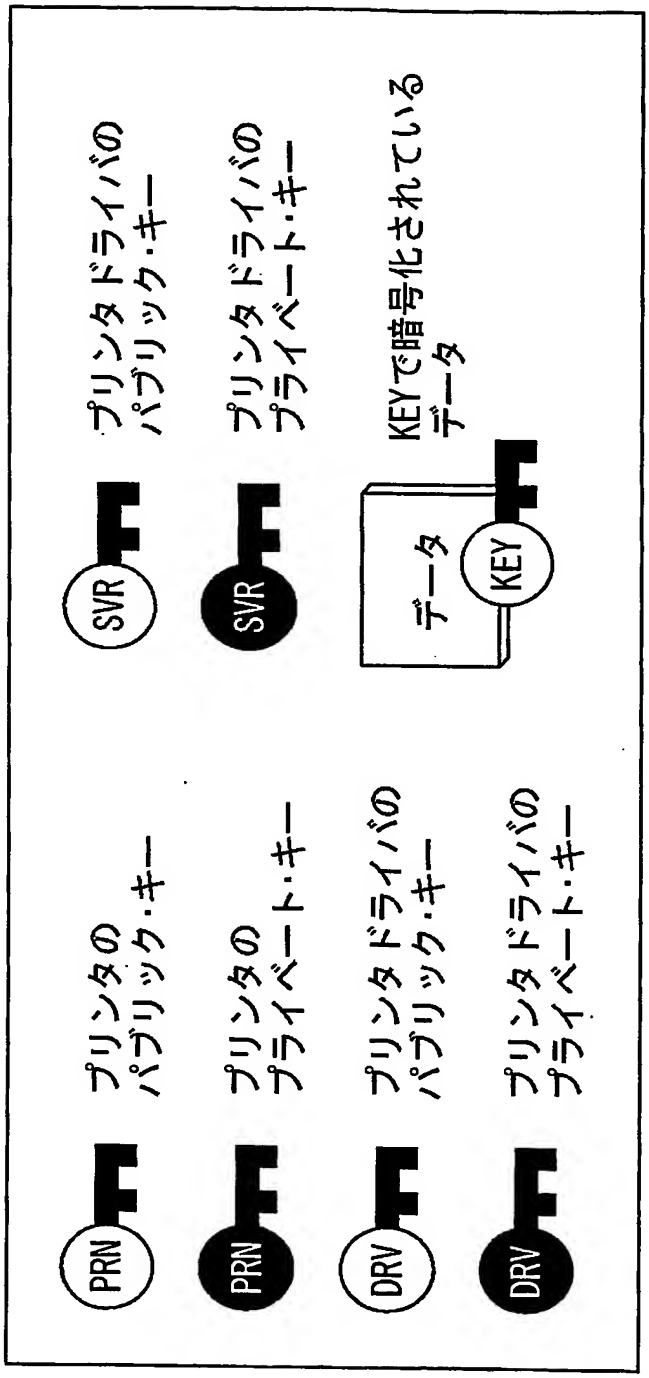
【図１２】


4000
35
CPU
RAM
プログラム ROM
NIC
31
32
33
34
100
3000
KB
CRT
外部メモリ (HD,FD)
9
10
11
2000
KBC
CRTC
DKC
PRTC
5
6
7
8
4
CPU
RAM
フォント ROM
プログラム ROM
データ ROM
3
1
2
3a
3b
3c
1500
21
印刷部
外部メモリ (HD,ID)
操作部
17
22
1000
入力部
印刷部 I/F
MC
18
16
20
15
CPU
RAM
フォント ROM
プログラム ROM
データ ROM
14
12
13
14a
14b
14c

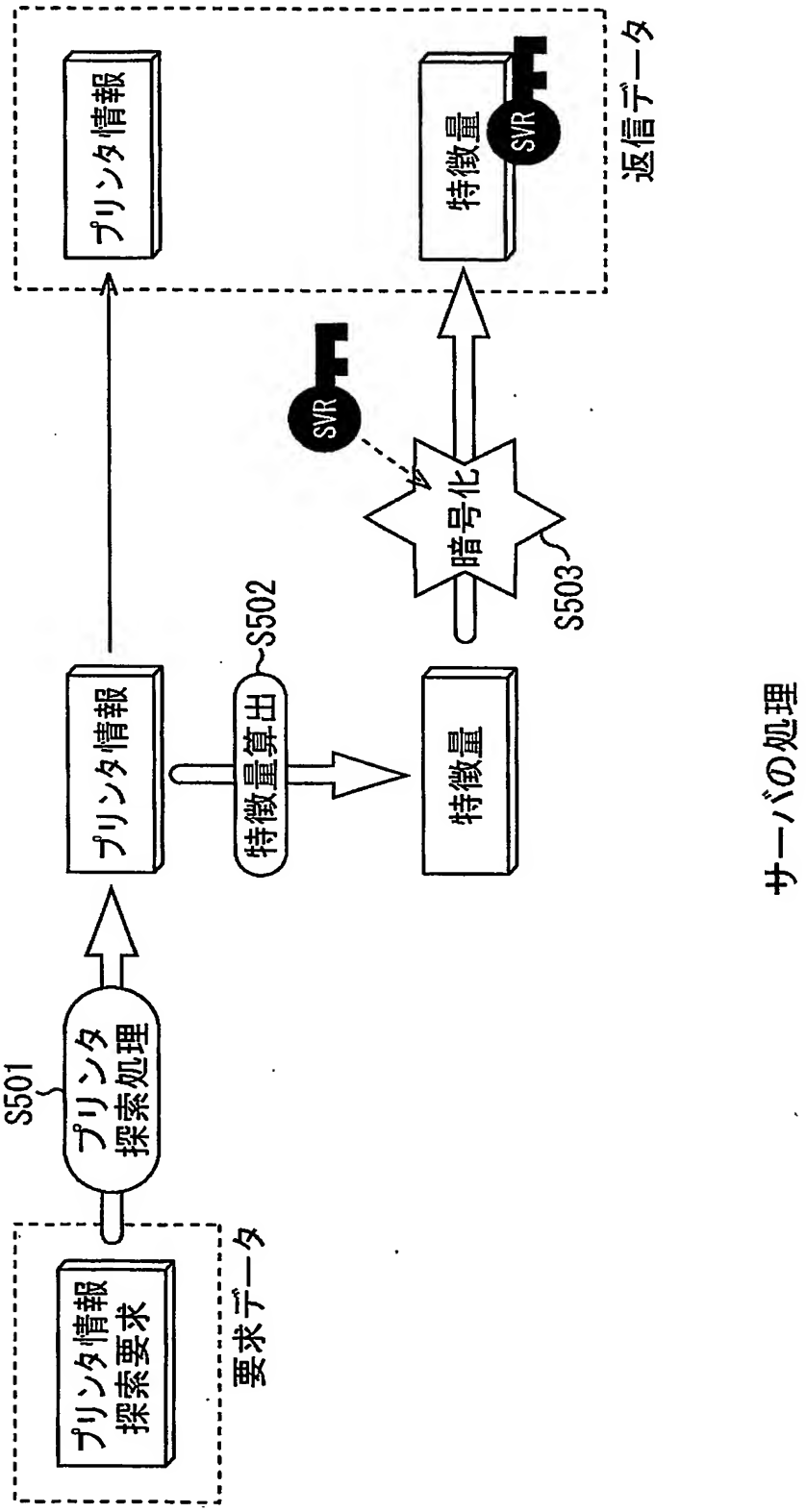
【図１３】


(a)ホストコンピュータ
アプリケーション
空きメモリ
関連データ
印刷処理
関連プログラム
OS
BIOS
301
302
303
304
305
306
(b)プリンタ管理サーバ
空きメモリ
関連データ
サーバ処理
関連プログラム
OS
BIOS
311
312
313
314
315
(c)プリンタ
空きメモリ
関連データ
印刷処理
関連プログラム
OS
BIOS
321
322
323
324
325

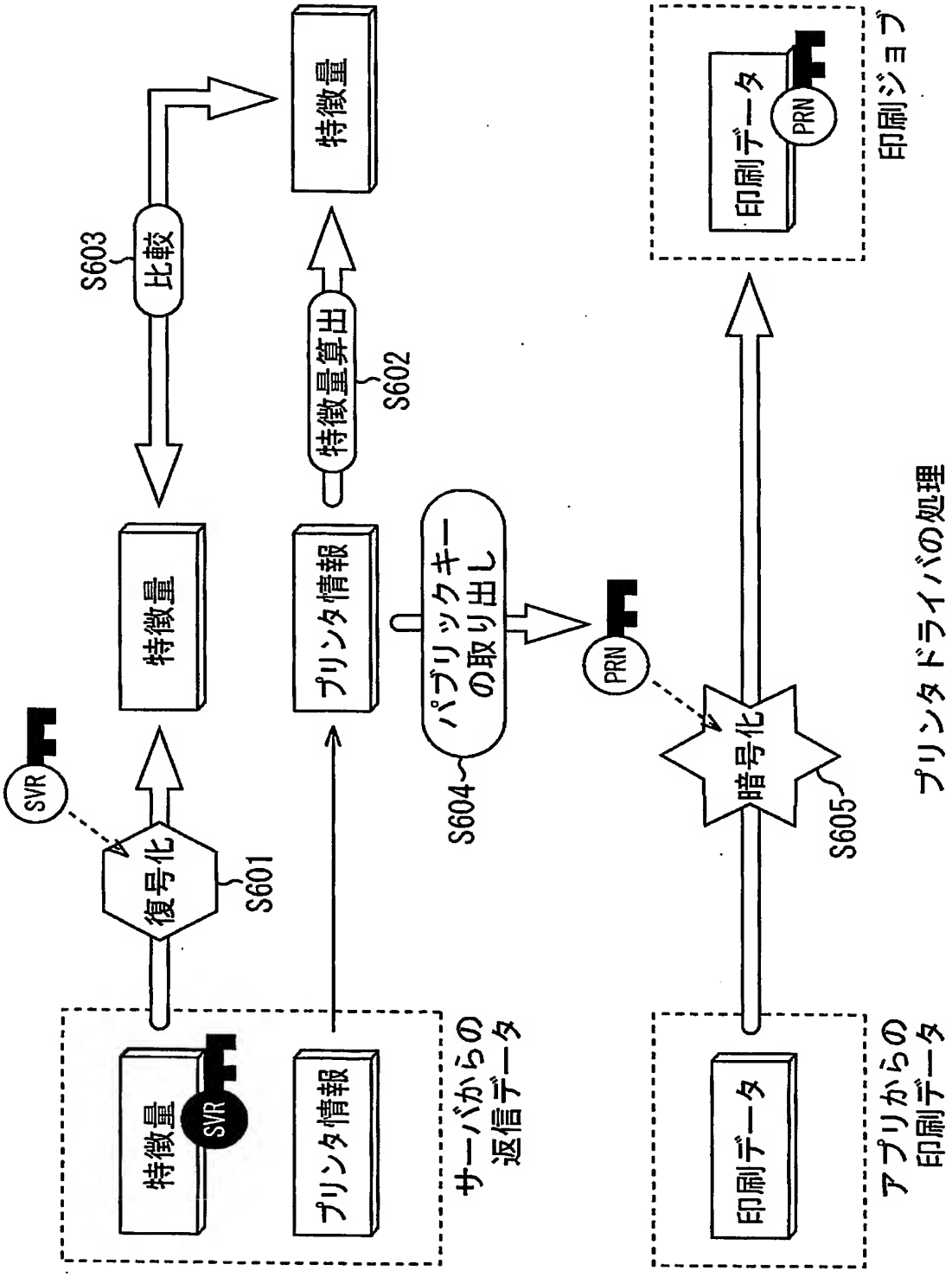
【図１４】


プリンタドライバの
パブリック・キー
プリンタドライバの
プライベート・キー
KEYで暗号化されている
データ
SVR
SVR
データ
KEY
プリンタの
パブリック・キー
プリンタの
プライベート・キー
プリンタドライバの
パブリック・キー
プリンタドライバの
プライベート・キー
PRN
PRN
DRV
DRV

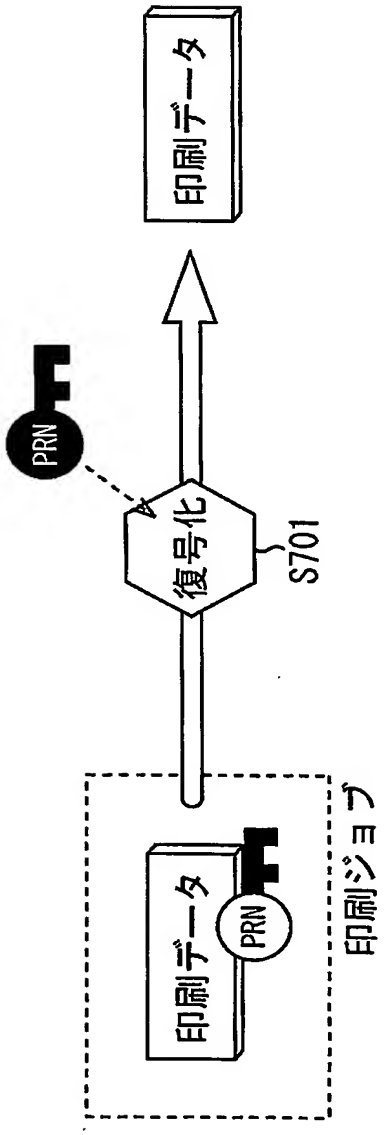
【図１５】


プリンタ情報
特徴量
SVR
返信データ
SVR
暗号化
S503
S502
プリンタ情報
特徴量算出
特徴量
サーバの処理
S501
プリンタ
探索処理
プリンタ情報
探索要求
要求データ

【図１６】

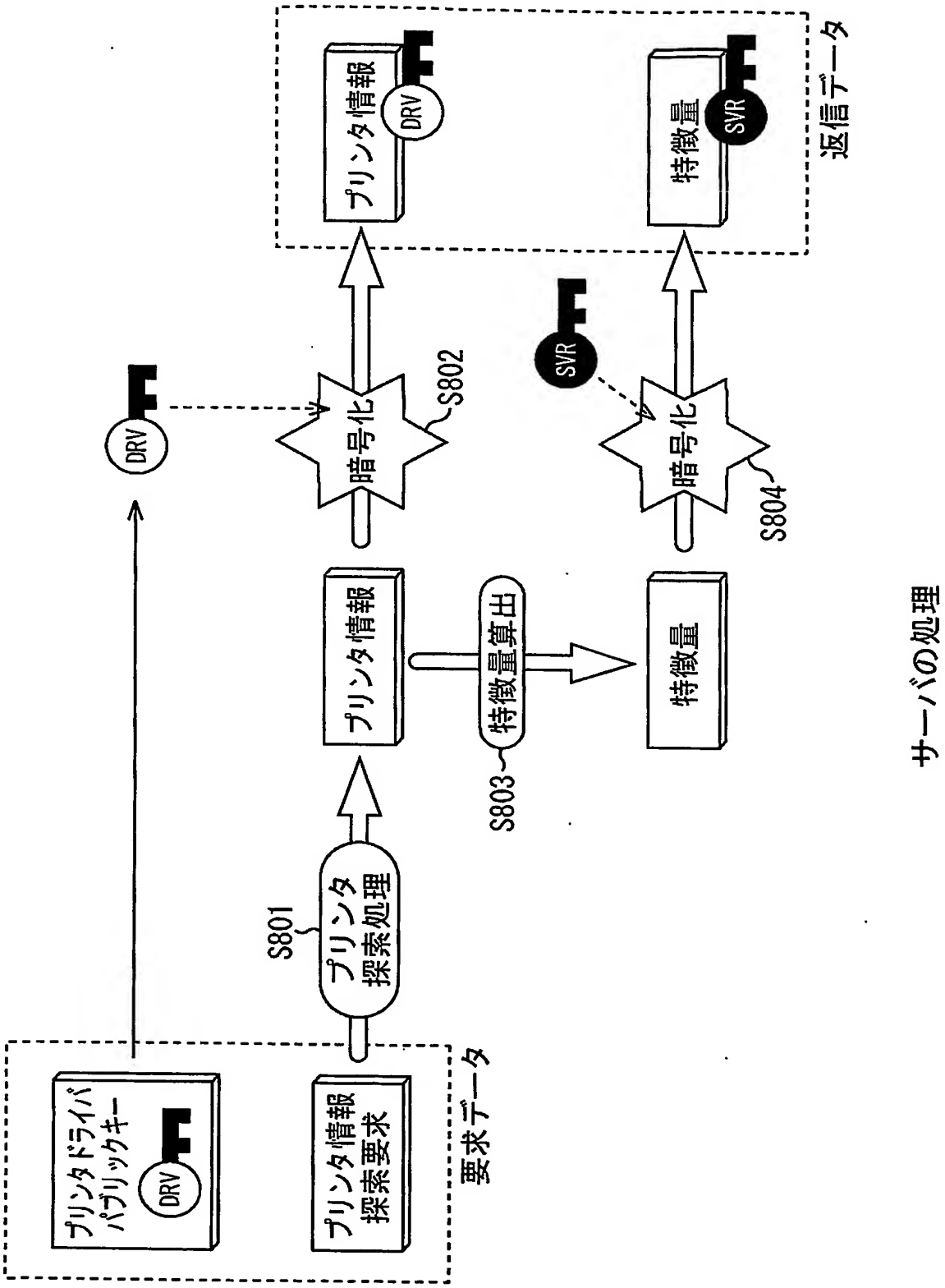

プリンタドライバの処理
サーバからの返信データ
特徴量
SVR
プリンタ情報
アプリからの印刷データ
印刷データ
PRN
印刷ジョブ
S601
復号化
S602
特徴量算出
S603
比較
S604
パブリックキーの取り出し
S605
暗号化

【図１７】

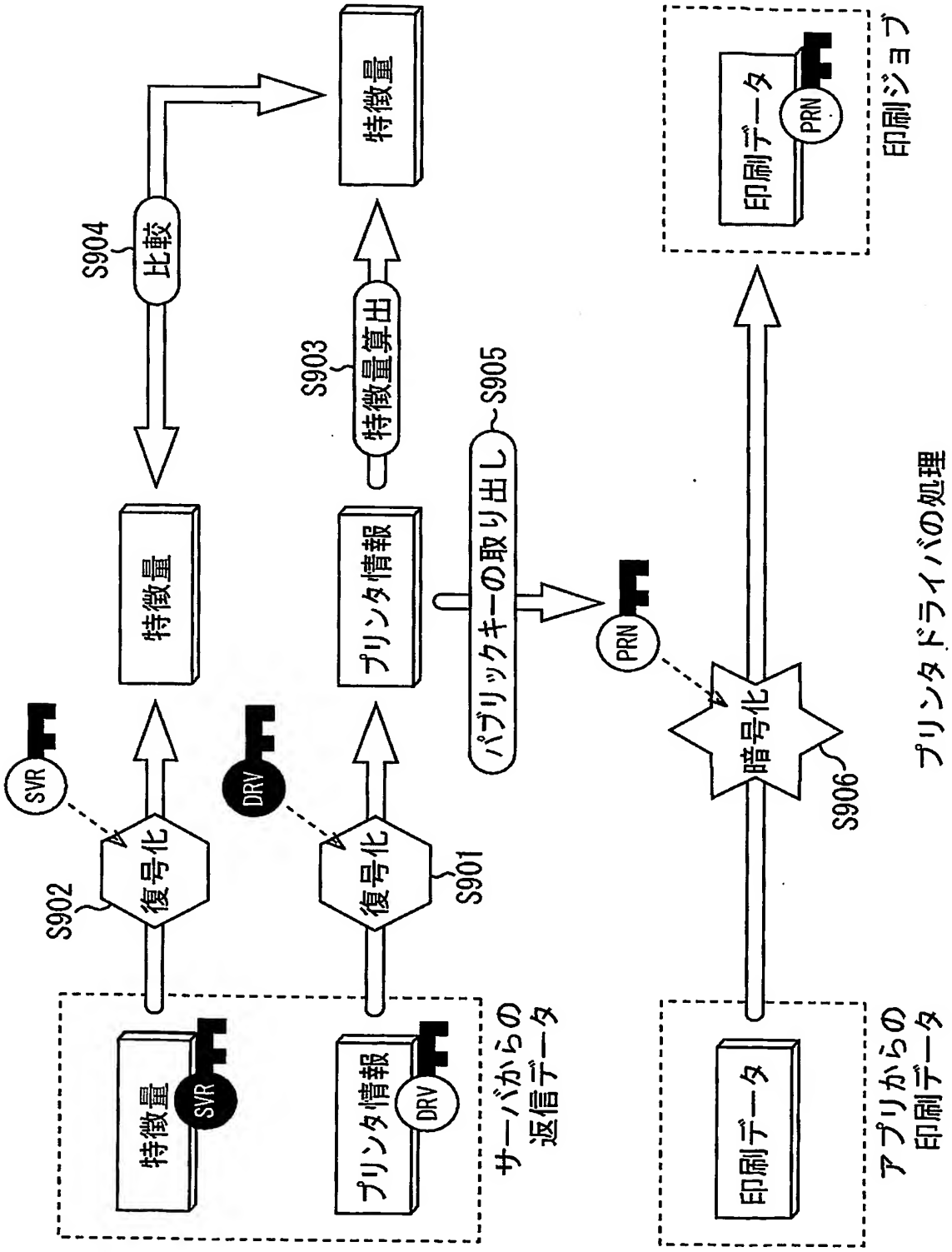


プリンタの処理

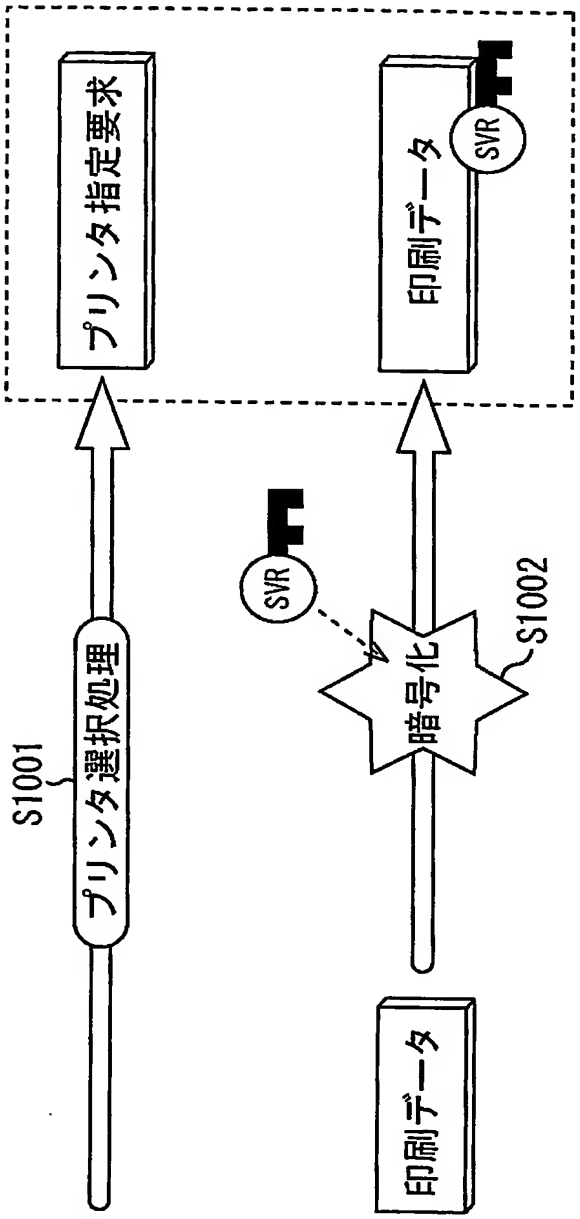
【図１８】


プリンタドライバ
パブリックキー
DRV
プリンタ情報
探索要求
要求データ
S801
プリンタ
探索処理
プリンタ情報
特徴量算出
特徴量
S803
DRV
暗号化
S802
SVR
暗号化
S804
プリンタ情報
DRV
特徴量
SVR
返信データ
サーバの処理

【図１９】

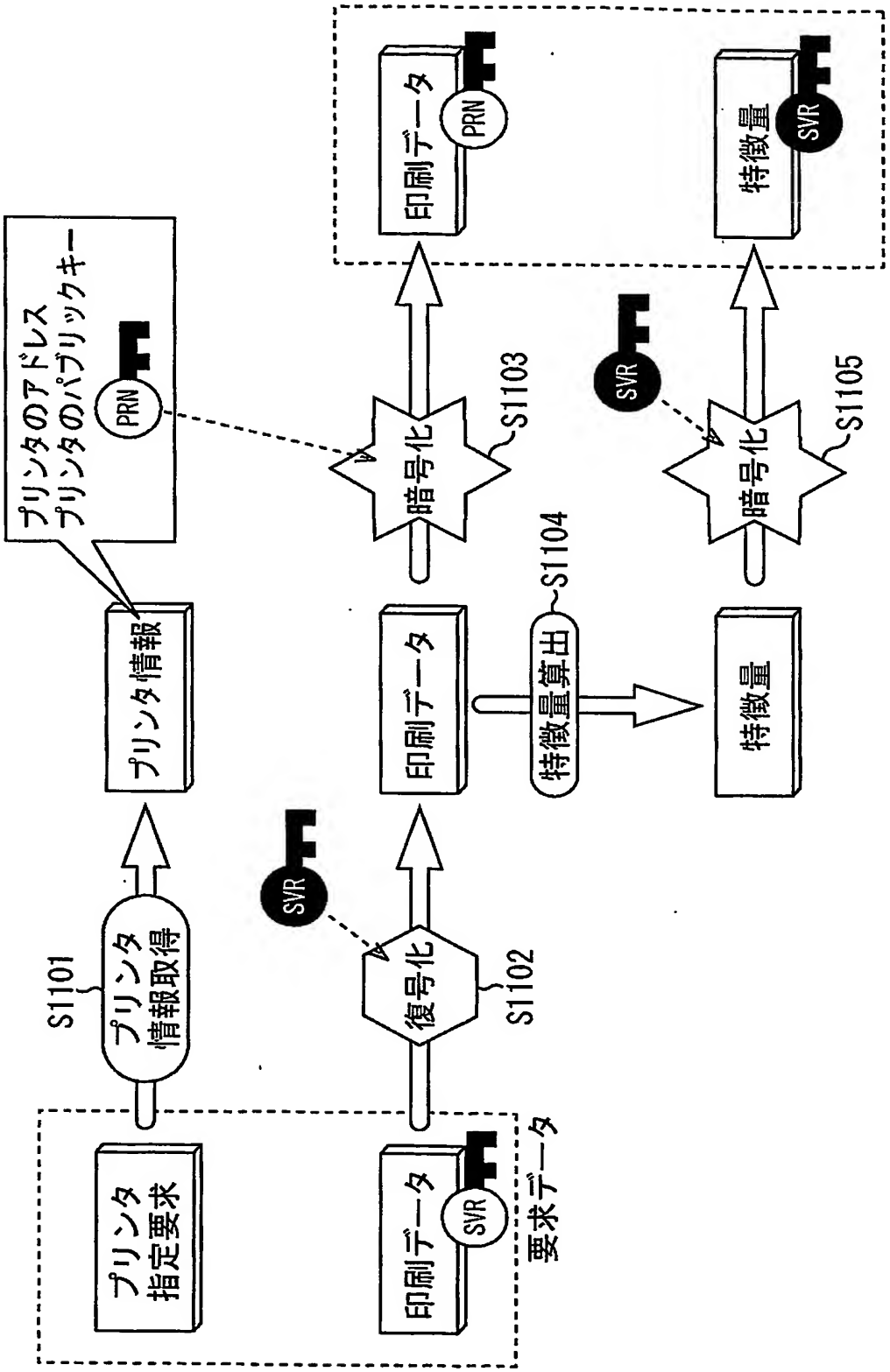

サーバからの返信データ
アプリからの印刷データ
プリンタドライバの処理
印刷ジョブ
特徴量
SVR
復号化
S902
プリンタ情報
DRV
復号化
S901
特徴量算出
S903
比較
S904
パブリックキーの取り出し
S905
PRN
暗号化
S906
印刷データ
PRN

【図２０】

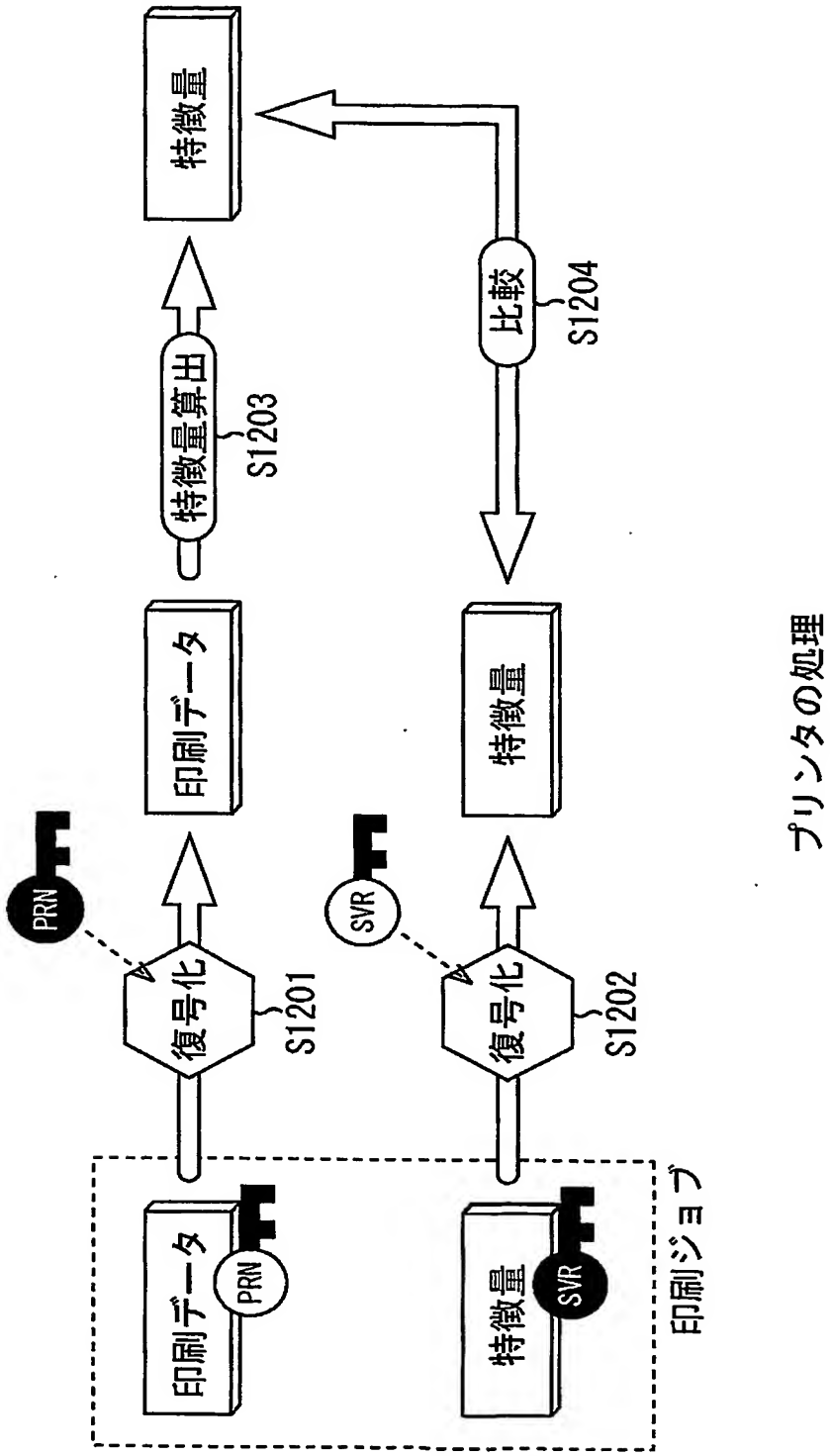


プリンタドライバの処理

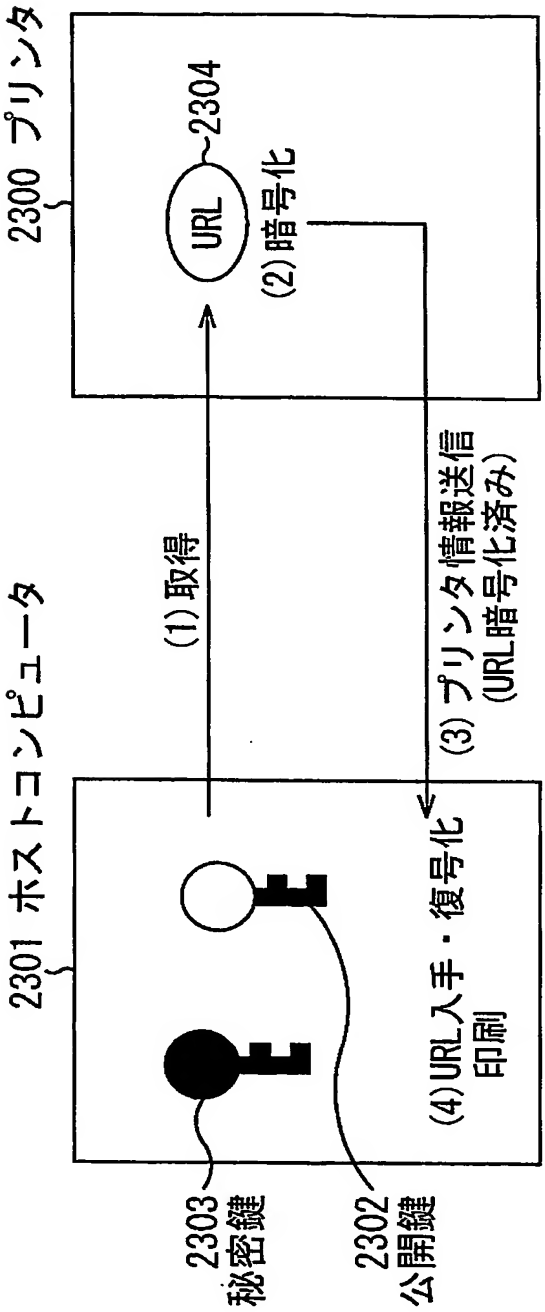
【図２１】


プリンタのアドレス
プリンタのパブリックキー
PRN
プリンタ情報
プリンタ
指定要求
S1101
プリンタ
情報取得
SVR
復号化
S1102
印刷データ
SVR
要求データ
印刷データ
暗号化
S1103
PRN
印刷データ
S1104
特徴量算出
特徴量
SVR
暗号化
S1105
特徴量
SVR
サーバの処理

【図２２】


印刷ジョブ
印刷データ
PRN
特徴量
SVR
復号化
S1201
復号化
S1202
印刷データ
特徴量
特徴量算出
S1203
比較
S1204
特徴量
プリンタの処理

【図２３】


2300 プリンタ
URL
2304
(2) 暗号化
(1) 取得
(3) プリンタ情報送信
(URL暗号化済み)
2301 ホストコンピュータ
(4) URL入手・復号化
印刷
2303
秘密鍵
2302
公開鍵

【書類名】要約書
【要約】
【課題】　ネットワークやインターネットを経由して印刷を行なう際に、印刷データが盗み取られたとしても、前記盗み取られた印刷データが第三者に利用されてしまうことを可及的に防止することができるようにする。
【解決手段】　ホストコンピュータ３０００のプリンタドライバは、アプリケーションから印刷要求を受けて印刷データを受け取ると、その印刷データを送信先のプリンタ１５００のパブリックキーで暗号化してプリンタ１５００に送信し、プリンタ１５００が、受信した印刷ジョブ中の印刷データをプライベートキーで復号化して印刷データを取得するようにすることにより、他のプリンタでは印刷データを復号化することができないようにして、たとえネットワーク１００上で印刷データを盗み取られたとしても、その印刷データが他のプリンタで印刷されてしまうことを防止できるようにする。
【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－２８０３７５
受付番号	５０３０１２３６４６０
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　８月　１日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000001007
【住所又は居所】	東京都大田区下丸子３丁目３０番２号
【氏名又は名称】	キヤノン株式会社

【代理人】　申請人

【識別番号】	100090273
【住所又は居所】	東京都豊島区東池袋１丁目１７番８号　池袋ＴＧホーメストビル５階　國分特許事務所
【氏名又は名称】	國分　孝悦

特願２００３－２８０３７５

出　願　人　履　歴　情　報

識別番号　　［０００００１００７］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社